DM

Avaliação de Segurança Informática numa Instituição Pública

DISSERTAÇÃO DE MESTRADO

Carolina Mendonça de Sousa
MESTRADO EM ENGENHARIA INFORMÁTICA

UNIVERSIDADE da MADEIRA
A Nossa Universidade
www.uma.pt

março | 2023

Avaliação de Segurança Informática numa Instituição Pública

DISSERTAÇÃO DE MESTRADO

Carolina Mendonça de Sousa
MESTRADO EM ENGENHARIA INFORMÁTICA

ORIENTAÇÃO
Eduardo Miguel Dias Marques

Faculdade de Ciências Exatas e da Engenharia

Mestrado em Engenharia Informática

Avaliação de Segurança Informática numa Instituição Pública

Carolina Mendonça de Sousa

Orientado por:

Eduardo Miguel Dias Marques

14 de março de 2023

Resumo

A Cibersegurança vem a ser cada vez mais utilizada com o desenvolver e a integração da tecnologia no dia a dia das pessoas, seja para trabalho como vida pessoal. No contexto de Cibersegurança a Engenharia Social é um dos tipos de ataque mais utilizados, sendo que os atacantes aproveitam-se das vulnerabilidades dos utilizadores para ter sucesso. O *phishing* é o método de engenharia social mais comum, este visa a recolha de informações das vítimas. Outro método de ataque utilizado são os dispositivos *USB* maliciosos, que contêm *malware* com o objetivo de difundi-lo e/ou de danificar os dispositivos.

Considerando o uso destes ataques é relevante saber o quão vulneráveis as pessoas realmente estão, se existem fatores que afetam a perceção sobre os ataques, e se fornecer recursos para educar as pessoas é significativo para o aumento dos conhecimentos. É importante os utilizadores aprenderem a reconhecer e qual o procedimento a ter em situações de *phishing* e de dispositivos *USB* de fontes desconhecidas. Este conhecimento é transmitido através de campanhas de consciencialização e permite a proteção de dados no trabalho e na vida pessoal.

O projeto, aqui apresentado, tem como objetivo a educação dos membros de uma comunidade académica sobre engenharia social (focando no *phishing* e em *pens* maliciosas), através de uma campanha de consciencialização. Para verificar a eficácia da campanha, foram feitos ataques simulados antes e depois da desta, e através dos resultados de ambos os ataques e da sua comparação, procurar identificar o grau de melhoria (ou não) da consciência das pessoas para a cibersegurança.

A pouca quantidade de resultados no caso de estudo com as *pens USB* não permitiu fazer uma análise que pudesse avaliar o impacto na comunidade académica. Já a análise e comparação dos resultados do caso de estudo do *phishing* possibilitou identificar alguns dos comportamentos de risco por parte de diferentes membros da universidade e permitiu uma melhor adequação da formação em cibersegurança. A análise aos dados de ambas as campanhas mostrou uma vulnerabilidade relevante em todos os grupos, tendo em ambos os ataques, e.g., mais de 50% de ligações maliciosas selecionadas. Outro fator relevante identificado, foi o fator idade nos alunos, sendo os alunos de menor idade mais vulneráveis e este ataque, identificados como os alunos dos cursos técnicos e 1º ciclo (geralmente, idades entre 18 e 21 anos). No geral, concluiu-se que a formação necessita ser melhorada de forma a reduzir estas vulnerabilidades.

Keywords: engenharia social · consciencialização · *phishing* · *USB*

Abstract

Cybersecurity is being used more and more with the development and integration of technology in people's daily lives, whether for work or personal life. In the context of Cybersecurity, Social Engineering is one of the most used types of attack, with attackers taking advantage of user vulnerabilities to succeed. Phishing is the most common method of social engineering, it aims to collect information from victims. Another attack method used is malicious USB devices, which contain malware with the aim of spreading it and/or damaging the devices.

Considering the use of these attacks, it is relevant to know how vulnerable people really are, if there are factors that affect the perception of attacks, and if providing resources to educate people is significant for increasing knowledge. It is important for users to learn how to recognize and what to do in situations of phishing and USB devices from unknown sources. This knowledge is transmitted through awareness campaigns and enables data protection at work and in personal life.

The project, presented here, aims to educate members a academic community about social engineering (focusing on phishing and malicious pens), through an awareness campaign. To verify the effectiveness of the campaign, simulated attacks were made before and after the campaign, and through the results of both atacks and their comparision, seek to identify the degree of improvement (or not) in people's awareness of cybersecurity.

The small amount of results from the attack with pens did not allow for an analysis that could evaluate the academic community. The analysis and comparison of the phishing results made it possible to assess some of the risky behaviours by different members of the university and allowed a better adequacy of training in cybersecurity. The comparison between both campaigns showed a relevant vulnerability in all groups, in both attacks, e.g., more than 50% of malicious links clicked. Another relevant factor identified was the age factor in the students, with younger students being more vulnerable to this attack, identified as students of technical courses and 1st cycle (generally, ages between 18 and 21 years old). Overall, it was concluded that training needs to be improved in order to reduce these vulnerabilities.

Keywords: social engeneering · awareness · phishing · USB

Agradecimentos

Agradeço à Infopédia, ao Priberam e ao Sinónimos.

Agradeço também a todos os que me acompanharam nestes anos de licenciatura e mestrado, dentro e fora da universidade.

Conteúdo

Lista de Figuras

Lista de Tabelas

1 Introdução

A Cibersegurança é um conceito cada vez mais importante em diversas áreas, seja na área governamental, empresarial ou em atividades pessoais do dia a dia [1]. Esta é referida em diversos campos, como o de engenharia de software, o de relações internacionais, o de gestão de crises e o de segurança pública.

Apesar da importância do conceito, ainda não há uma definição abrangente e uniforme [2], visto o significado de Cibersegurança depender, muitas vezes, do contexto e de situação em que é aplicado, tornando-o subjetivo. Esta ambiguidade desencadeia limitações em avanços científicos e tecnológicos [3].

Com o objetivo de encontrar uma definição uniforme, Craigen *et al.* [3], realizaram uma revisão da literatura e discutiram o tema com profissionais, estudantes e académicos. A definição à qual chegaram através da escrita do artigo 'Defining Cybersecurity' foi a seguinte:

> *"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."*
>
> "Cibersegurança é a organização e o conjunto de recursos, processos e estruturas usadas para proteger o ciberespaço e os sistemas habilitados para o ciberespaço, de ocorrências que desalinham o *de jure* do *de facto* nos direitos de propriedade, do *de facto*."

Esta definição abrange não só os aspetos técnicos, como também aspetos externos à tecnologia, tais como os comportamentos e as vulnerabilidades dos humanos, sendo que ambos são as bases da engenharia social [4]. É importante ter atenção ao aspeto humano, que muitas vezes é ignorado pelos responsáveis pela segurança, a favor dos aspetos técnicos [5].

O método para combater as vulnerabilidades dos utilizadores é educar os mesmos sobre a Cibersegurança, mais especificamente, sobre engenharia social e sobre vários meios de ataque, através de campanhas de consciencialização. Neste trabalho irão ser focados os ataques de *phishing* e ataques via *pens USB*.

Os ataques de *phishing* são comunicações falsificadas que tentam enganar o humano fazendo-se passar por fontes fidedignas, através de por exemplo: *e-mails*, chamadas e mensagens. Os atacantes tentam recolher dados pessoais ou credenciais para ganhos financeiros ou para ter acesso a recursos de interesse.

As *pens* maliciosas são usadas para a instalação de *malware* nos dispositivos. Através da instalação deste tipo de *software* os dispositivos são danificados ou desabilitados, os atacantes podem beneficiar com dados recolhidos nestes aparelhos, ou fazer com que estes deixem de poder realizar as suas tarefas.

Na realização destes ataques, para fins de estudo, e para a campanha de consciencialização são usados alguns recursos do Kit MetaRed, fornecidos pela própria iniciativa MetaRed. Este é um projeto colaborativo de países pertencentes à Ibero-América. Em Portugal, este projeto é desenvolvido por instituições de ensino público e privado, com o objetivo de aumentar a divulgação na área de TICs (Tecnologias da Informação e Comunicação).

1.1 Contexto

A campanha de consciencialização teve lugar na Universidade da Madeira (UMa), durante o ano letivo de 2021/2022 e teve como alvo os membros da comunidade académica. Para esta campanha foram identificados três grupos principais, funcionários, docentes/investigadores e estudantes.

Esta divisão deve-se ao facto de as pessoas pertencentes a cada grupo terem funções/objetivos diferentes consoante o seu papel na UMa, o que significa que os dados e as informações a que têm acesso também são diferentes. Os docentes e investigadores foram considerados um só grupo por haver maior sobreposição de algumas pessoas com cargos em ambos os grupos.

Os alunos são o grupo com acesso a informação mais limitado, sendo que cada aluno apenas tem acesso à sua conta. Os funcionários e docentes/investigadores são os grupos com acesso a informação mais sensível. Apesar desta diferença é importante que todos os grupos sejam educados em relação à segurança, tanto para evitar o roubo de dados pessoais e outras informações relativas à UMa, como para evitar que os computadores (ou outros dispositivos) pessoais e da universidade sejam comprometidos.

1.2 Metodologia

Como referido anteriormente, o método escolhido para educar a comunidade académica foi uma campanha de consciencialização. Esta campanha é composta por três ações, o envio de *e-mails* informativos, a colocação de cartazes alusivos à Cibersegurança pela universidade, e uma ação de formação.

Para apoiar a campanha foram feitos dois tipos de ataques, antes e depois da campanha. Os ataques são de *phishing* e de *pens* USB. O ataque anterior à campanha não só serve para alertar as pessoas de como estão vulneráveis aos ataques como também para poder ser avaliado o nível de conhecimentos de como reconhecer e evitar o ataque. O segundo ataque, após a campanha, serve para avaliar se houveram alterações relevantes nos resultados, mostrando se a campanha foi eficaz ou não.

A campanha foi planeada de acordo com os resultados dos ataques, os métodos escolhidos variaram consoante os grupos de utilizadores, tendo em conta as necessidades de cada um.

O ataque de *phishing* foi feito através do envio de um *e-mail* elaborado de forma a incentivar as pessoas a interagir com este, havendo diferenças na mensagem dependendo do grupo ao qual o destinatário pertence. O ataque via *pens USB* realizou-se ao espalhar as *pens* pela universidade, com ficheiros maliciosos disfarçados, dando falso sentido de confiança a quem as encontrar, incitando-as a abrir os ficheiros.

1.3 Objetivos e Questões

Este projeto visa, sobretudo, a fornecer conhecimentos a todos os membros da comunidade académica mediante uma campanha de consciencialização, de forma a sensibilizá-los sobre a engenharia social, os diferentes tipos de ataque e como os reconhecer, afim de evitar ser vítima, impedindo a exposição de dados ou informação sensível.

Usando os dois métodos de engenharia social, o *phishing* e as *pens* maliciosas, foram feitos ataques simulados à comunidade académica da UMa com o objetivo de avaliar o quão sensibilizados

estão os membros dos vários grupos da universidade. A realização de dois ataques, antes e depois da campanha, e da comparação de resultados, tem como finalidade aferir se uma campanha de consciencialização é eficaz.

Para além da campanha, os ataques são feitos com o intuído de poder analisar os resultados para responder a algumas questões baseadas nos parâmetros escolhidos.

Com os resultados dos ataques de *phishing*, poderão ser analisados alguns parâmetros, para perceber se são relevantes aquando da avaliação dos conhecimentos de cada grupo. Para os funcionários foi analisado se o serviço em que trabalham influencia os resultados. Os parâmetros para os docentes/investigadores são as faculdades e centros de investigação, a que pertencem. E para os alunos é possível ter mais parâmetros para análise, estes são faculdade e escola, ciclo e ano.

Foram escolhidos analisar os serviço, as faculdades e escolas com a intenção de perceber se existem áreas profissionais ou de estudo em que as pessoas estão melhor informadas sobre engenharia social, e que as ajude a reconhecer quando são alvo de uma ataque. Os ciclos e os anos para os estudantes, podem indicar se o tempo que uma pessoa pertence a uma instituição, ou se a idade, assumindo que os anos e ciclos mais baixos correspondem a pessoas mais novas, altera a perceção sobre o tipo de *e-mails* que são enviados.

Para os ataques com *pens* USB as perguntas de interesse são se algum dos grupos é mais vulnerável ao ataque, se as pessoas interagem com o conteúdo da *pen* e se ao interagir há algum tipo de ficheiro que as pessoas estão mais propensas a abrir.

1.4 Organização do Documento

Este documento está dividido em cinco capítulos e as suas secções. Após a introdução inicia-se o Estado de Arte (2), onde são apresentadas definições detalhadas de engenharia social, de *phishing* e de ataques via *USB*. Seguem-se as secções onde são caracterizados os casos de estudo sobre o conhecimento dos dois tipos de ataque, começando com o conhecimento sobre *Pens USB* (3) seguido do conhecimento sobre *phishing* (4). Nestas secções é explicado como foram feitos os ataques, são apresentados os resultados e a sua análise, e ainda na secção de *phishing* (4) é descrita a campanha de consciencialização. No último capítulo são apresentadas as conclusões (5) e o trabalho futuro.

2 Estado de Arte

Este capítulo serve para apresentar os conceitos relevantes para esta dissertação. São dadas definições de engenharia social e *phisihing*, e são descritos os vários tipos de ataques de *phishing* e via *USB*. Também são referidos os métodos aconselhados para a consciencialização dos utilizadores sobre engenharia social e a prevenção dos vários tipos de ataque. A caracterização dos meios para educar e dos ataques é significativa para a compreensão da campanha e dos ataques realizados como parte deste projeto.

A Engenharia Social é o acto de manipular e/ou enganar uma pessoa, ou um grupo de pessoas, levando-a a partilhar informação sensível ou usando-a para obter dinheiro ou outros benefícios e, onde conseguir a confiança da(s) vítima(s), é o mais importante para um atacante [6, 7].

Na Cibersegurança, a Engenharia Social é a forma de ataque com mais peso, comparando-a com outras ameaças, e sendo uma das mais fáceis, mais baratas e mais eficientes de implementar [7]. Os atacantes aproveitam-se das vulnerabilidades comuns do ser humano e este, muitas das vezes, torna-se o elo mais fraco num sistema de informação. Através de interações sociais os atacantes influenciam, persuadem, manipulam e induzem as vítimas a revelar informação [8].

No contexto da Cibersegurança a definição de Engenharia Social está sempre a mudar de modo a incluir novos métodos de ataque [9]. Estes novos métodos de ataque são consequência da evolução tecnológica, sendo que atualmente os seres humanos dependem da tecnologia tanto para o trabalho como para a vida pessoal, aumentando as opções dos atacantes para explorar as vulnerabilidades dos seres humanos.

Devido há existência de vários métodos de como realizar um ataque de Engenharia Social, e de que as definições que existem podem referir-se a apenas um ou a vários métodos de ataque, para este projeto foi decidido usar a definição proposta por Wang *et al.* [9]. Esta definição não depende do tipo de ataque e tem em conta outras definições encontradas na literatura e é apresentada de seguida, de forma origicanl e traduzida para português:

> *"In the context of cybersecurity, social engineering is a type of attack wherein the attacker(s) exploit human vulnerabilities by means of social interaction to breach cyber security, with or without the use of technical means and technical vulnerabilities."*
>
> "No contexto de Cibersegurança, engenharia social é o tipo de ataque onde o(s) atacante(s) exploram vulnerabilidades humanas através de uma interação social para quebrar a Cibersegurança, com o uso ou sem o uso de meios técnicos ou vulnerabilidades técnicas."(tradução do autor)

Como referido anteriormente, o ser humano é o elo mais fraco a ter em conta no que toca à proteção de uma rede ou da informação duma empresa, instituição ou organização. É necessário perceber que, embora a parte técnica da segurança é importante e necessita de estar bem desenvolvida, estes sistemas não são capazes de proteger-se daquilo que parece ser um acesso autorizado [10, 11].

Os atacantes, também conhecidos como engenheiros sociais, têm como objetivo manipular a pessoa a divulgar informação sensível, usando truques psicológicos, destacando-se os seguintes: aproveitar-se do comportamento da pessoa após apresentar um contexto com aparência normal, apresentar mensagens falsificadas, mas com imagens/logótipos bem conhecidos ou explorar a previsibilidade das respostas das pessoas em algumas situações sociais [11]. Isto é possível ao aproveitar as emoções e os sentimentos de uma pessoa para ganhar a confiança desta [8]. O engenheiro social

não tem de ser alguém proficiente em tecnologia, especificamente informática, apenas tem de conseguir persuadir a pessoa, ou grupo de pessoas, através de comportamentos e de crenças durante as suas interações [10].

As vulnerabilidades exploradas em engenharia social, para além das emoções (e sentimentos), são: cognição e conhecimento, comportamento e hábito e fatores psicológicos. Estes últimos ainda podem ser divididos em: natureza humana, traços de personalidade e características individuais [8].

Na implementação das várias técnicas de Engenharia Social foi identificado um padrão comum nos seus processos ([6], [7], [10]), e identificado em quatro passos, representados na Figura 1. O primeiro é a recolha de informação, seguida do estabelecimento de uma relação e confiança e, no passo seguinte, com a exploração dessa relação, concluindo com a execução do ataque e possível benefício para o atacante. Estes passos podem ter um ou vários ciclos para o atacante conseguir os seus objetivos.

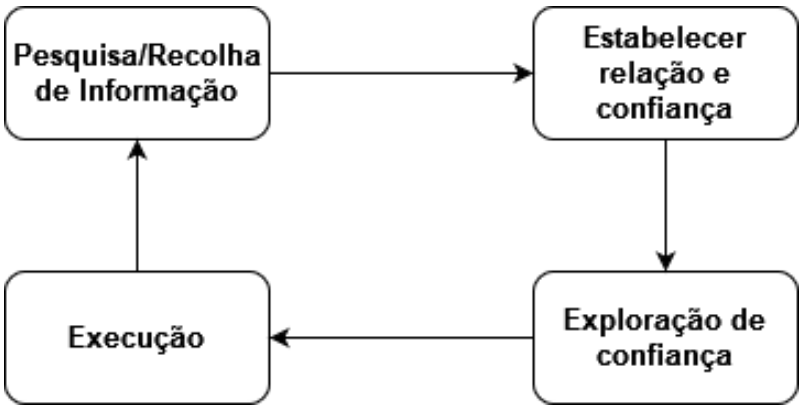

Figura 1: Diagrama de passos no processo de um ataque de Engenharia Social [6, 7, 10].

Os passos de um ataque são usados nos diferentes métodos de ataque de Engenharia Social, que podem ser realizados com o uso ou sem o uso de tecnologia. Os métodos de ataque são os seguintes:

- *Phishing* - uso de meios de comunicação, como *e-mails*, mensagens diretas, chamadas e *SMSs*, para enganar a vítima de forma a que esta partilhe informação ou instale *software* malicioso [8, 10, 11];
- *Water-holing* - o atacante descobre os *websites* acedidos regularmente pelas vítimas, infeta-os com código malicioso, e espera que as vítimas interajam com este, transferindo o código malicioso ou carregando em ligações maliciosas [8];
- *Pretexting* - o atacante fabrica uma história (quanto mais complexa, melhor) e representa um papel falso para que a vítima acredite que este é de confiança, criando ainda um sentido de urgência de modo a que a vítima não tente verificar se a história é real, e assim responda logo, divulgando dados sensíveis ou outra informação requerida pelos atacantes [10];
- *Quid pro quo* - há uma troca de informação ou serviços entre o atacante e a vítima, pois o atacante faz-se passar por um assistente técnico e oferece-se para ajudar a vítima, mesmo quando não há nada de errado procurando obter informação privada [10];

- *Baiting* - o atacante oferece algo à vítima, normalmente bens ou informação, esperando da parte da vítima acesso a informação ou de alguma ação por parte da vítima que permita outros ataques. Um exemplo é deixar uma *pen USB* com código malicioso num sítio frequentado pela vítima, em que o exterior da *pen* seja algo que provoque curiosidade à vítima e a leve a inserir no seu computador para saber o que esta contém [8, 10];
- *Tailgaiting/Piggybacking* - estando no mesmo sítio, o atacante segue a vítima até a zona a que quer aceder e à qual a vítima tem acesso, por exemplo: portas com acesso por cartão [8, 11];
- *Shoulder surfing* - olhar para o ecrã onde a vítima está a inserir as credenciais privadas com o objetivo de as ver e memorizar, sem que esta se aperceba [11];
- Manipular a conversa - fazer com que as conversas sejam sobre o tópico de segurança, para que as pessoas comecem a revelar informação sensível. Um caso possível poderia ser o atacante falar sobre os seus dados de acesso (falsos ou inventados) e tentar que a vítima, em troca, indique as suas credenciais, por abuso de confiança [8].

Algum destes métodos podem ser usado utilizado individualmente ou vários podem ser utilizados conjuntamente para atacar o mesmo alvo. Como nem todos estes ataques usam tecnologia, podem ser realizados por pessoas com poucos conhecimentos tecnológicos, aumentado assim o número de possíveis engenheiros sociais e, em consequência, ataques.

As secções seguintes, 2.1 e 2.2, descrevem dois tipos de ataques que, embora usem aspetos tecnológicos, utilizam as abordagens de Engenharia Social referidas na sua execução. Os atacantes usam o *phishing* e os ataques via dispositivos *USB*, pois estes tomam proveito das vulnerabilidades dos humanos para que tenham sucesso. Ainda, na secção 2.3, são discutidos os métodos para prevenir este tipo de ataques.

2.1 *Phishing*

O *phishing* é um tipo de ataque de Engenharia Social que tem como principal objetivo enganar a vítima, através de uma mensagem maliciosa, para que esta partilhe informação sensível. O primeiro ataque de *phishing* registado e divulgado aconteceu em 1995 e ocorreu na plataforma AOL através de mensagens instantâneas e de *e-mails* [12–15].

É um tipo de ataque antigo mas, continua a ter sucesso ao longo dos anos e até aos nossos dias, havendo ainda uma tendência para o aumento da frequência deste tipo de ataques devido aos atacantes continuamente inventarem novas formas de o executar [12, 16]. O *Anti-Phishing Working Group*[1] (APWG) publica relatórios com as estatísticas de ataques de *phishing* ao longo do ano, e, embora só contabilize os ataques reportados, podemos ver nas Figuras 2a e 2b o aumento da quantidade de ataques de um ano para outro e a confirmação da tendência referida (linha a tracejado azul em ambas as imagens).

O gráfico da Figura 2a apresenta três linhas, uma com o número de ataques referentes a *websites* de *phishing* (linha azul), ou seja, o número de *websites* falsos usados para *phishing*, cada *website* conta como um ataque. Uma linha em relação aos ataques por *e-mail* (linha laranja), cada frase no campo de assunto diferente conta como um ataque. E ainda a linha de tendência (linha a tracejado azul).

[1] https://apwg.org/

(a) 2020 [17]. (b) 2021 [18].

Figura 2: Ataques de *phishing* reportados à APWG

Já o gráfico da Figura 2b apresenta duas linhas, linha referente ao número de *websites* de *phishing* (linha vermelha), e a linha de tendência (linha a tracejado azul). Ao comparar os dois gráficos, o número de *websites* não só aumenta durante o ano, como entre os dois anos também aumentou. Enquanto que em 2020 o valor mais alto de ataques foi acima de 200 000, em 2021 o valor mais alto foi acima dos 300 000.

É de notar que em 2020 houve um aumento nos ataques e no número de vítimas de *phishing*, em relação a anos anteriores, durante a pandemia de COVID-19, porque aumentou o número de pessoas a usar serviços *online*, seja para trabalho ou lazer, o que fez com que deparassem-se com mais esquemas fraudulentos [19].

Neste artigo, a definição de *phishing* a ser considerada foi a de Lastdrager [20], pois esta não define o *phishing* baseando-se apenas no meio em que os ataques são difundidos. É também uma definição considerada em outros trabalhos, como [13, 15, 21]. A definição é a seguinte:

> *"Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target."*
>
> "*Phishing* é um ato escalável de enganar, onde a personificação é usada para obter informação de um alvo."(tradução do autor)

Tendo em conta esta definição, várias técnicas de *phishing* são utilizadas para atacar as possíveis vítimas e a utilização das diferentes técnicas depende dos recursos, dos objetivos e do tipo de informação que o atacante consegue recolher antes de realizar o ataque. As formas de ataque são:

- *Phishing* - apesar de *phishing* ser usado como nome que engloba vários tipo de ataques, tem origem nos ataques feitos através de *e-mails*, sendo este o método mais usado para realizar os ataques [22]. O atacante cria uma mensagem fraudulenta fazendo-se passar por uma entidade ou por outra pessoa, de forma a que a vítima partilhe informação ou dados privados [23].
- *Spear phishing* - feito da mesma forma que *phishing* e com o mesmo objetivo, é um ataque direcionado a um indivíduo, ou grupo específico que tenha algo em comum, (por exemplo: funcionários da mesma empresa), normalmente os alvos são empresas [21, 23];
- *Whaling* - tal como *spear phishing* é um ataque direcionado, mas o indivíduo ou grupo são pessoas com os cargos de nível mais alto na empresa [23];

- *Smishing* - a vítima recebe SMSs que se fazem passar por algum serviço relevante à vítima, podendo conter um *link* para um *site* falso ou pedir para enviar informação privada [21];
- *Vishing* - através de chamadas ou mensagens de voz, os atacantes fazem-se passar por empresas ou instituições e pedem informação privada [21];
- *Phishing clone* - copiar um *website* em que a vítima confia, para que esta insira as suas credenciais e o atacante possa guardá-las [22, 23];
- *Pharming* ou *DNS phishing* - aproveita as vulnerabilidades do *DNS* e redireciona a vítima para uma cópia do *website* ao qual esta tentava aceder. Para alterar o mapeamento do *DNS* pode ser via a implementação de código malicioso no servidor *DNS* [22, 23];
- *Man-in-the-middle* - o atacante interceta mensagens e altera-as durante a transmissão entre o remetente e o destinatário [22, 23].

Existindo várias técnicas que podem ser implementadas ao realizar um ataque de *phishing*, a implementação destas técnicas consiste em três elementos: meio, vetor e abordagem técnica. Estes elementos, que podem ser combinados entre si para desenvolver os vários tipos de ataque, caracterizam-se da seguinte forma [12, 13]:

- Meio - modo pelo qual o atacante interage ou comunica com a vítima, é a base para conseguir levar o ataque até ao alvo. O desenvolvimento tecnológico tem aumentado a quantidade de meios de comunicação, tornando-se mais fácil contactar as vítimas, exemplos: chamadas, SMSs, *internet* [12, 13];
- vetor - é o canal que o atacante tem para levar o ataque à vítima e depende do meio, i.e., se o meio é chamadas o vetor é *vishing*; se o meio é SMSs o vetor é *smishing*; se o meio for a *internet* os vetores são por exemplo: *e-mails*, *websites*, mensagens diretas [12, 13];
- Abordagem técnica - é a utilização de um ou mais vetores, em conjunto com engenharia social, para realizar o ataque. Embora sejam menos populares, existem ataques de *phishing* em que a sua abordagem não incluí engenharia social, por exemplo: injeção SQL, *sound-squatting* e *typo-squatting* [12,13]. A abordagem técnica é o que define um ataque e, como mencionado anteriormente, pode ser a combinação de vários vetores, por exemplo: enviar um *e-mail*, fazendo-se passar por um serviço, que contém uma ligação para um *website*, que se parece com o *website* real do serviço, afim de conseguir as credenciais ou outras informações da vítima. O envio de *e-mails* e de mensagens instantâneas e o uso de *sites* falsos são o primeiro, segundo e terceiro métodos mais populares de *phishing*, respetivamente [23].

Considerando o *phishing* como um ataque de Engenharia Social, é necessário perceber quais os fatores humanos a influenciar o seu sucesso. Desolda *et al.* [21] realizaram uma revisão da literatura e chegaram à conclusão que os fatores humanos com maior contribuição para uma maior vulnerabilidade são:

- Falta de conhecimento - os utilizadores não são educados nos temas de Cibersegurança, nem como evitar ataques em contexto pessoal ou profissional;
- Falta de recursos - a falta de ferramentas, aplicações, abordagens e *frameworks* para ajudar na educação dos utilizadores. Não há um padrão para a criação destas, tornando-se muito específicas porque, normalmente, são criadas para um determinado grupo de pessoas;

- Falta de consciência (*lack of awareness*) - os utilizadores não prestam a devida atenção às suas ações e, se houver uma mudança simples ou mais elaborada nas ações do dia-a-dia, como na introdução de credenciais, no caso de um ataque, por vezes, não reparam ou ignoram as diferenças nas suas ações;
- Normas - alguns hábitos menos seguros seguidos ao longo do tempo dentro da organização podem representar uma vulnerabilidade. Os utilizadores novos, e mesmo os mais antigos, tendem a adotar comportamentos semelhantes aos dos colegas de trabalho, mesmo que estes sejam perigosos;
- Complacência - os utilizadores têm dificuldade em alterar comportamentos habituais, sentindo-os como seguros e subestimando os possíveis perigos.

O método mais recomendado para evitar este tipo de ataques é ensinar os utilizadores a reconhecê-los e a evitar interagir com qualquer tentativa de *phishing* [11, 13, 24]. Isto é importante para empresas, instituições e organizações, pois possuem muitos dados sensíveis e os ataques poderão ter um maior impacto.

Outro tipo de ataque comum em empresas, instituições e organizações, são os ataques via dispositivos *USB*, falados na secção seguinte (2.2).

2.2 Ataque via *USB*

As tecnologias *USB* foram adotadas em grande escala em 2003, tornando-se assim uma superfície de ataque bastante popular e, desde então, apareceram imensos riscos de segurança associados a estas tecnologias [25, 26]. Os atacantes escolhem este meio de ataque porque os periféricos *USB* são acessíveis, baratos e *plug and play* (não necessitam instalação) [27]. Também pelo facto do sistema operativo não fazer a autenticação do controlador do dispositivo, possibilitando o atacante de disfarçar o dispositivo [26].

Os ataques via dispositivos *USB* são muito explorados na área de Sistemas de Controlo Industrial (SCI) [28]. Esta área lida com infraestrutura essenciais como a gestão da água, a produção e distribuição da eletricidade, as redes de transportes, as operadoras de comunicações e os organismos de saúde, e em todos eles as *pen drives* são, regularmente, muito usadas para transferência de dados dentro e entre instituições [27]. Embora muitos dos dispositivos destas áreas operem de forma isolada, seja fisicamente ou em redes isoladas e mesmo através de *firewalls* para os salvaguardar, o uso de *pen drives* torna o isolamento pouco eficaz e facilmente ultrapassado [28].

O ataque via *USB* mais mediático ocorreu em 2010 no ataque à Central Nuclear Natanz no Irão, com a instalação de um *worm* designado de Stuxnet. Apesar de esta Central operar numa rede isolada da Internet, o código malicioso foi introduzido através de uma *pen drive* infetada, usada para a transferência de dados entre um sistema externo exposto à Internet e outro interno. O código malicioso só era ativado quando inserido no seu alvo, no entanto espalhou-se além dos dispositivos *USB*, através da partilha de impressoras e vulnerabilidades de privilégios. Este ataque provou que o uso de dispositivo *USB* era eficiente em ataques, mesmo quando a rede de uma empresa é uma rede local isolada [29].

Os ataques via *USB* podem ser feitos em duas direções, de um periférico *USB* comprometido para o *host* (por exemplo: de um rato para um computador), ou de um *host* comprometido para

um periférico *USB* (*pen drive*) [30]. Os vários tipos de ataques via *USB* podem ser organizados nas seguintes categorias:

- *Malware* guardado em dispositivos *USB* de armazenamento externos. Este método permite que o código malicioso seja difundido por vários dispositivos [27];
- Dispositivos U3 são reconhecidos como CD-ROM, desta forma podem usar a função *auto-run* para executar código malicioso [27, 30];
- *USB in the Middle* - dispositivo instala *loggers* de atividade, por exemplo: *keyloggers, printer loggers, USB sniffers* [27];
- Dispositivos de *DNS USB* tentam interromper o serviço de duas formas: atacando diretamente o *host* (por exemplo: *USB-killer*), ou infetando vários dispositivos e estes fazem o ataque de *DNS* [27];
- *HIDs (Human Interface Devices) USB* (por exemplo: teclados, ratos) podem ser reprogramados, embutindo o *firmware* de um dispositivo com código malicioso [27, 30];
- *USB killer* é uma *pen* que ao conectar a uma entrada *USB* carrega um condensador, e depois liberta essa a energia acumulada no dispositivo, o ciclo repete-se até o dispositivo alvo ser incapacitado [30].

Embora a maioria dos ataques via *USB* necessitem de Engenharia Social para serem implementados [30], a grande parte das soluções aconselhadas são de aspeto técnico, ou seja, afetam só o software e não são uma solução universal [25–28].

O uso da Engenharia Social acontece devido ao facto dos utilizadores confiarem que os dispositivos *USB* vão fazer apenas a tarefa que o utilizador quer, quando na realidade o dispositivo está infetado [30]. Também porque ao encontrarem uma *pen*, muitas vezes, acabam por introduzi-la no seu computador, fazem-no por curiosidade ou motivos altruístas, com o objetivo de devolver ao dono [31].

Para testar se os utilizadores realmente introduzem uma *pen* nos seus dispositivos e abrem os seus ficheiros, foi feito um estudo [31] na Universidade de Illinois[2]. O estudo passou, inicialmente, por deixar 297 *pens* em vários sítios do campus universitário. Para perceber as ações das pessoas que utilizaram a *pen*, após introdução desta no computador e a abertura de um ficheiro, os utilizadores eram redirecionadas para um questionário e, para incentivá-las a responder, eram oferecidos dez dólares. No final do estudo os resultados obtidos indicaram que mais de 45% das *pens* foram abertas e que 98% foram recolhidas pelos utilizadores.

O método para prevenir este tipo de ataques, tal como outros tipos de ataques de Engenharia Social, é através da educação dos utilizadores na área da Cibersegurança e da engenharia social [29]. A secção seguinte apresenta algumas abordagens para a prevenção de tipo de ataques através da educação dos utilizadores.

2.3 Educar e Conscienciализar

Os métodos identificados como mais eficientes na prevenção dos ataques de Engenharia Social, complementando os processos técnicos, são as campanhas de consciencialização sobre segurança da informação e os programas de treino, ambos devendo ser feitos regularmente. As empresas cada

[2] https://illinois.edu/

vez mais investem nestas campanhas e treinos para os seus funcionários, sabendo que estes são o elo mais fraco da segurança pela sua falta de conhecimento no tema [32–34].

Ambos os métodos podem ser feitos em separado, mas têm mais efeito quando aplicados em conjunto. As campanhas servem para educar as pessoas sobre os tipos de ataque, que informação põe em risco ao serem vítimas, quais as informações que os diferentes dispositivos guardam, de que formas estão vulneráveis e a reconhecer mensagens e comunicações enganosas. Os programas de treino ajudam a que as pessoas reconheçam os ataques e quais os procedimentos a ter durante ou, se tendo sido atacado com sucesso, após o ataque. Este programas permitem e recomendam a prática regular com o conteúdo fornecido e atualizado [33, 35].

Para prevenção dos ataques de *phishing* uma das abordagens mais referidas é o treino integrado, isto é, fazer ataques simulados de *phishing* e complementar com material de treino e material informativo. O material de treino, normalmente são jogos, mas enquanto uns defendem estes serem eficientes em familiarizar as pessoas com situações que possam ocorrer no dia a dia, outros defendem que os exemplos não são representativos do tipo de ataques reais [33,35–37]. O material informativo pode ser em formato de vídeo, *e-mails*, *blogues*, panfletos, cartazes e sessões de formação [33, 34, 36, 38]. Para as sessões de formação não só é necessário um especialista da área para ensinar os conceitos, também é benéfico aos participantes a partilha das suas experiências [37].

Embora a educação também seja aconselhada para evitar os ataques de *pens* (ou outros dispositivos *USB*), não existem métodos específicos no contexto de ataques de Engenharia Social, sendo a maior parte dos métodos de prevenção através de soluções técnicas [39]. Não podendo evitar o uso destes dispositivos, a solução aconselhada é educar os utilizadores para saber usar os programas que analisam os dispositivos e a saber interpretar os resultados [40].

No entanto existem dificuldades ao tentar implementar os métodos referidos:

- Economia - as empresas podem não ter a capacidade financeira para implementar as campanhas e treinos, regularmente ou até mesmo uma só vez [32];
- Interesse - por mais material que seja disponibilizado, mesmo que em diferentes formatos, as pessoas podem não ter interesse em aprender [32, 38];
- Perceção - mesmo pessoas dos mesmos grupos ou áreas profissionais, estas interpretam as informações de formas diferentes, sendo difícil de garantir a passagem dos conhecimentos a todos da mesma forma [32];
- Tempo - é preciso tempo para aprender sobre o tema, quer seja no trabalho ou na vida pessoal, as pessoas podem não estar dispostas a ceder o seu tempo [32];
- Horário - outro aspeto do tempo é coordenar as sessões entre as várias pessoas, visto todas terem horários diferentes, não é eficiente fazer muitas sessões com um número reduzido de pessoas, em vez de poucas sessões com mais pessoas [32];
- Comportamento - a base da Engenharia Social é o comportamento humano e, assim, é difícil que a informação passada em campanhas, normalmente muito genérica para chegar à maioria das pessoas, possa ser específica para cada pessoa, pois cada pessoa tem reações diferentes a diferentes situações e conteúdos [32, 38];

– Modo de educar não presencial - caso seja escolhido implementar métodos onde não há interação direta entre o instrutor e as pessoas que estão a ser educadas, por exemplo: vídeos, texto; quem está a aprender pode não ter forma de expor as suas dúvidas [38].

Mesmo com estas dificuldades, a abordagem de treino integrado ainda é vista como favorável para prevenir os ataques. Desta forma há uma maior possibilidade de educar os utilizadores sobre os conceitos no contexto de Engenharia Social e os procedimentos a tomar na suspeita de ataque [41].

2.4 Conclusões

A Engenharia Social é um aspeto da Cibersegurança com cada vez mais relevância, o que significa que os responsáveis pela segurança em instituições, empresas e organizações precisam de se focar mais no aspeto humano da segurança.

Um dos ataques que mais explora as vulnerabilidades humanas é o *phishing*, maioritariamente usado para conseguir das vítimas dados e informações privadas.

O outro ataque explorado é feito através de dispositivos *USB*, onde um *malware* é lá inserido e procura chegar a computadores e/ou servidores. Além da introdução de código malicioso com objetivos diversos, este método é mais usado para desabilitar *hardware*.

Para combater os ataques que usam a Engenharia Social é necessário educar os utilizadores para os seus perigos e para conhecer as suas formas de prevenção.

No geral, durante a pesquisa para estes temas foi fácil encontrar informação quanto aos seus conceitos, à sua evolução e a forma que estes são vistos atualmente. No entanto aquando da pesquisa dos métodos de prevenção, embora a consciencialização e a educação fossem os métodos mais referidos, é difícil encontrar artigos que relatem casos específicos.

Nos artigos em que tal foi referido, descrevendo a aplicação dos métodos de educação e indicando o seu sucesso, não era apresentado o contexto nem os dados dos resultados dessas ações, procurando clarificar alguns dos aspetos desses trabalhos. Se para o ataque via *pens USB* apenas foi encontrado um artigo, no caso do ataque de *phishing* não foi possível encontrar trabalhos com dados detalhados.

3 Caso de Estudo: *Pens USB*

Neste capítulo é explicado o caso de estudo de ataques via *pens USB*, começando com uma introdução ao caso de estudo, seguida do plano (3.1) e da implementação (3.2), onde é descrita a preparação do ataque. Após estas duas secções são apresentados os resultados (3.3) e são feitas as conclusões (3.4) sobre o estudo.

O ataque via *pens* foi realizado ao espalhar *pens USB* no edifício da universidade, situado na Penteada, não foram espalhados dispositivos em outras localidades como o Colégio dos Jesuítas ou a Residência Universitária. As *pens* contem ficheiros disfarçados, que ao serem abertos redirecionam para uma página *web* de consciencialização, que permite saber que alguém interagiu com as *pens*.

Durante o planeamento deste ataque foi tido em conta a descrição deste tipo de ataque simulado do Kit MetaRed e o ataque simulado descrito no artigo [31].

O objetivo com este ataque é aumentar o nível de consciencialização dos membros da comunidade académica, começando por avaliar o quão vulneráveis os utilizadores são a este ataque.

Para além do objetivo geral do projeto, existem algumas perguntas a responder com base neste ataque. A primeira seria se as pessoas realmente inserem a *pen* num computador (ou outro dispositivo) e o porquê de o terem feito. Verificar também se têm em conta o aspeto da *pen* e se influencia esta decisão, se ao inserirem a *pen*, interagem com o conteúdo da mesma, o porquê de o terem feito e se há algum tipo de ficheiro que as pessoas têm mais tendência a abrir.

Outra questão a responder é se existe algum grupo mais vulnerável a este tipo de ataques. Os grupos alvos são os três previamente mencionados (funcionários, docentes/investigadores e estudantes), com a adição do grupo visitantes, esta adição deve-se ao facto da universidade ser uma instituição pública, que permite o acesso às instalações àqueles que não fazem parte da mesma, não sendo possível certificar-se que só membros da universidade irão encontrar as *pens*.

Este ataque foi feito com o conhecimento da Instituição e, mais especificamente, da Unidade de Comunicações e Informática (UCI).

3.1 Plano

O caso de estudo de ataques via *pens* USB foi feito numa única fase, esta fase consistiu na preparação e na execução de um ataque. Este ataque serviu para avaliar a comunidade académica à sua possível vulnerabilidade, aproveitando para ao mesmo tempo educar as vítimas.

A preparação do ataque, consistiu na configuração das *pens*, preparação da página *web*, também consistiu na definição de parâmetros a analisar, em decidir o conteúdo das *pens*, na formulação de um questionário, e após o ataque, na análise dos resultados.

Para o caso de estudo de ataques via *pens* não houve uma segunda fase com campanha de consciencialização ou ainda um segundo ataque. Esta decisão deve-se ao facto de que o ataque foi feito numa dimensão muito menor, onde havia a possibilidade de que os resultados não fossem relevantes e que não fosse possível tirar conclusões através da sua análise.

3.2 Implementação

Foram preparadas oito *pens*, todas com aspetos diferentes. Cada *pen* foi identificada com um número, como se vê na Figura 3, desta forma seria possível distingui-las durante a preparação do ataque e durante a análise dos resultados.

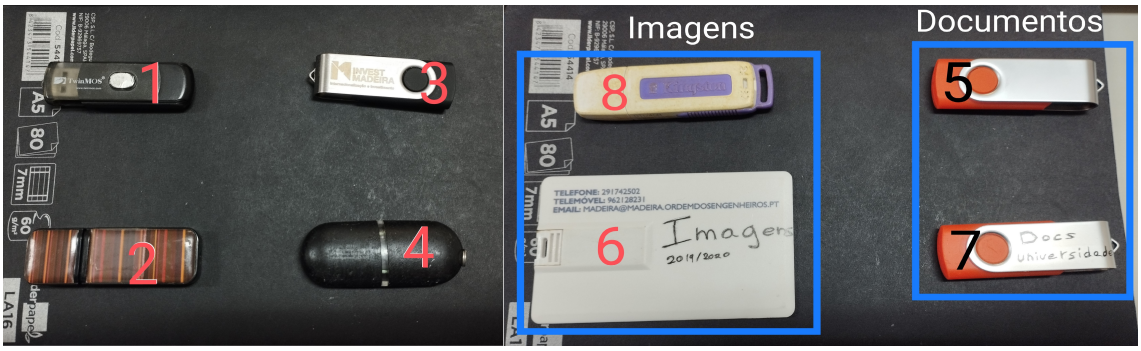

Figura 3: Identificação das *pens*.

Ainda para as *pens* 6 e 7 foi escrito o seu conteúdo no exterior, também para ver se o aspeto dos dispositivos influencia a pessoa a usá-los.

Para além dos números, as *pens* diferenciam no seu conteúdo, havendo três tipos de conteúdo, das *pens* 1 à 4 o conteúdo são ficheiros do tipo imagens (.png) e documentos (.docx e .pdf), das *pens* 5 e 7 o conteúdo são só ficheiros do tipo documentos, e as *pens* 6 e 8 o conteúdo são só ficheiros do tipo imagens. Estas extensões servem para disfarçar os ficheiros, que na realidade são do tipo *VBScript (Visual Basic Script)*, e que reencaminham a pessoa para um site após serem abertos. Também foram mudados os ícones para corresponder à extensão falsa.

A nomenclatura das pastas e ficheiros foi dada de maneira a se parecer o mais natural possível, para que a pessoa que a utilizasse sentisse-se segura quando tentasse abrir os ficheiros.

A estrutura do conteúdo das *pens* está representada na Figura 4. Esta distinção de ficheiros serve para ajudar a responder à pergunta se há algum tipo de ficheiro que as pessoas tem mais tendência a abrir. Para poder avaliar essa tendência, a ligação usada para redirecionar as pessoas à página *web* criada, tinha um *ID* baseado no número da *pen* e no tipo de ficheiro. A ligação é composta por um *URL* do domínio da universidade (http://orion.uma.pt/simpen) seguido do *ID* (por exemplo: /?6.pdf), assim no histórico de acessos à página seria possível identificar cada *pen* e ficheiros abertos (por exemplo: http://orion.uma.pt/simpen/?6.pdf).

Foi criada para este projeto uma página *web* de alerta (Figura 79 em anexo), com o objetivo de informar que a *pen* fazia parte de uma campanha de consciencialização e que não continha nenhum ficheiro malicioso, e ainda continha uma ligação que redirecionava a pessoa a um questionário. Para além disso informava a pessoa que podia devolver a *pen* aos perdidos e achados, ou voltar a colocá-la em qualquer outro sítio da universidade para voltar a ser encontrada por outras pessoas.

O questionário (Anexo 5.1) , também criado para este projeto, consistia em perguntas para caracterizar a pessoa, como idade, género, estatuto em relação à universidade e a área/curso/serviço a que pertence; perguntas sobre onde encontrou e porque inseriu a pen num dispositivo; e perguntas

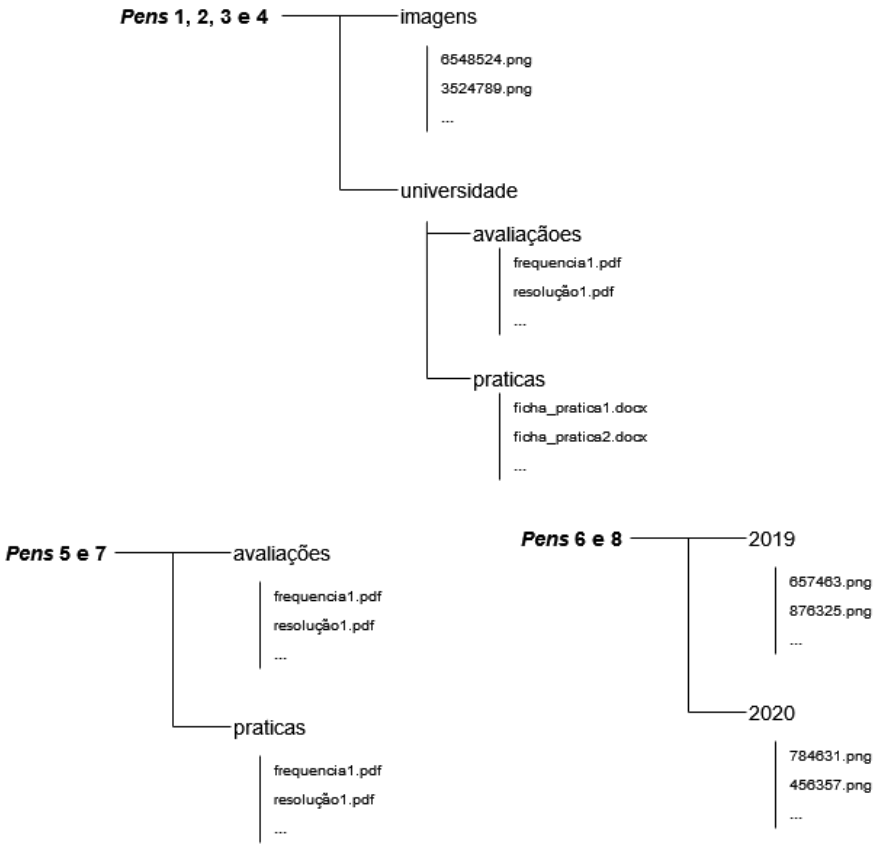

Figura 4: Estrutura do conteúdo das *pens*.

para caracterizar os seus conhecimentos de Cibersegurança, especificas sobre engenharia social e dispositivos *USB*.

Havendo a possibilidade das pessoas que encontraram as *pens* quererem entrega-las aos perdidos e achados da universidade, situado na entrada principal, mesmo sem ver a página informativa, foi pedida a colaboração dos serviços responsáveis pela gestão do edifício, desta forma os dispositivos *USB* entregues, poderiam voltar a ser espalhados. Este serviço também contribuiu ao dar acesso às salas de aulas para poder colocar duas das *pens*.

Após preparar as *pens* estas foram espalhadas pela universidade em dois dias, 19 e 20 de Abril. No primeiro dia foram deixas quatro *pens* entre as 7h30 e as 8h, uma no parque de estacionamento interior, uma no corredor do piso -2, uma no bar e uma na cantina. No segundo dia foram deixadas cinco *pens* (uma foi devolvida no primeiro dia), três foram deixadas, outra vez entre as 7h30 e as 8h, nas salas de estudo dos pisos 1, 2 e 3. As restantes *pens* foram deixadas nas salas de aulas 25 e 30, às 13h.

Os locais foram escolhidos por serem alguns dos mais frequentados, principalmente por alunos, sendo o parque de estacionamento o único mais utilizado por funcionários e docentes/investigadores.

O uso das *pens* foi monitorizado até o dia 5 de Maio, durante duas semanas, usando o histórico de acesso ao domínio "orion.uma.pt".

Ao longo da campanha e dos ataques aconteceram situações que durante o planeamento não foram consideradas, e por isso não se tornaram parâmetros/questões a responder ao longo do projeto, e que mesmo depois de deparar-se com elas, nem todas foram analisadas. Também houve situações que embora tenham sido consideradas, não poderiam ser controladas, e ainda situações que só foram notadas após os ataques. No entanto são aqui referidas para ter em conta em possíveis trabalhos futuros.

Considerando que os dispositivos *USB* usados estão configurados como *Pen Drive*, não é possível corre-los automaticamente nos sistemas operativos tidos em conta (Windows e macOS), desta forma não há maneira de verificar se houveram pessoas que inseriram a *pen*, mas não abriram nenhum ficheiro.

Outro facto a ter em conta são os dispositivos usados para abrir as *pens* não estarem conectados à *internet*, assim se os ficheiros foram abertos, não ficaram registados.

Por último, podemos assumir que todas as *pens* foram encontradas, visto não estarem mais nos sítios onde foram deixadas.

3.3 Resultados

Já mencionado anteriormente, uma das *pens* foi entregue aos perdidos e achados, não havendo registos de que algum ficheiro tenha sido aberto. Mais nenhuma *pen* foi devolvida.

Os outros resultados obtidos foram no dia 20 de abril, em que na *pen* 7 um ficheiro do tipo *PDF* foi aberto (Figura 5 linha 1), e no dia 4 de maio, na *pen* 2 um ficheiro do tipo *PNG* foi aberto (Figura 5 linha 2). Em nenhum destes casos o questionário foi respondido.

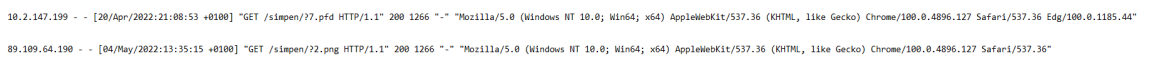

Figura 5: *Logs* de acesso à página *web* através dos ficheiros das *pens*.

Apesar de haver uma taxa de 22% de *pens* em que houve ficheiros que foram abertos, o facto de o número total de *pens* espalhadas ser tão pequeno (apenas 9), significa que não são resultados significativos.

3.4 Conclusões

Devido aos poucos resultados obtidos não é possível fazer uma análise que permita responder à maior parte das questões postas para este tipo de ataque. Podemos afirmar que as pessoas recolhem uma *pen* quando a encontram, mesmo sem nenhum indicativo de quem pertence ou do seu conteúdo, mas não temos informação sobre o motivo pelo qual fazem. Também podemos confirmar que há pessoas que introduzem as *pens* nos seus computadores (ou outros aparelhos que suportem estes dispositivos) e abrem os ficheiros, mas, mais uma vez, não temos informações sobre os seus motivos.

Havia a expectativa de conseguir uma maior reutilização de *pens*, contando que as pessoas quando as encontrassem as devolvessem ou redistribuíssem, visto o número de dispositivos ser tão pequeno no início. Num trabalho futuro deverão ser aplicadas mais *pens*.

4 Caso de Estudo: *Phishing*

Como mencionado no estado de arte de *phishing* (2.1), este é um tipo de ataque cada vez mais comum e tem como forma de prevenção recomendada o acompanhamento dos utilizadores relativamente ao seu conhecimento e à sua perceção sobre estes ataques e a área de Engenharia Social. Uma forma de acompanhamento pode ser através da realização de ataques controlados de *phishing*, ou seja, ataques simulados que nos permitem obter resultados e assim, poder antever qual o grau de abrangência de ataques reais, bem como as suas potenciais consequências.

O objetivo deste projeto é melhorar a consciência dos utilizadores pertencentes à instituição, sobre as abordagens de Engenharia Social, em particular os ataques de *phishing*, dando a conhecer os possíveis perigos caso sejam vítimas destes ataques, e os modos de os reconhecer e poderem defender-se contra os ataques.

A abordagem central deste projeto é a realização de ataques dirigidos a toda a comunidade académica, desde funcionários, docentes/investigadores e alunos, de modo a ter uma perceção completa dos conhecimentos sobre este tipo de ataque nos diferentes grupos. Após o primeiro ataque é feita a análise de resultados, esta é usada para definir as características da campanha de consciencialização, e quais os métodos que devem ser dirigidos a cada grupo. Por fim é feito o segundo ataque onde são comparados os resultados e é analisado o possível impacto da campanha de consciencialização.

Com uma amostra deste tamanho, existe a expectativa que os dados recolhidos sejam abrangentes e a sua análise permitirá tirar algumas conclusões sobre qual o grau de vulnerabilidade de cada grupo a este tipo de ataque, bem como apoiar na escolha das campanhas de consciencialização e avaliar a utilidade da campanha ao comparar os resultados dos ataques antes e depois.

Também existem algumas questões a responder que são mais específicas de cada grupo e, em cada grupo, serão analisados os resultados de entre diferentes categorias de membros. Os funcionários estão organizados em serviços, com maior ou menor exposição e experiência no uso do email. No caso docentes e investigadores, temos diversas faculdades/escolas e centros de investigação, de áreas muito distintas e será interessante perceber se existem diferenças na consciência sobre estes ataques. De forma similar, temos os alunos, além de estarem ainda divididos em diferentes ciclos de estudo. Os dados serão agrupados em diferentes categorias e poderão ajudar a perceber se existem (ou não) diferenças de atitudes e perceção para estes ataques.

Para o caso do *phishing* foram enviados *e-mails* em duas ocasiões diferentes, para os três grupos. As mensagens foram adaptadas para cada grupo, e para cada ataque.

É importante ainda referir que esta ação foi elaborada com o conhecimento e com a colaboração da Unidade responsável pelas comunicações digitais, fundamental para conseguir atingir toda a comunidade e com as devidas autorizações da Instituição. Foram ainda assinadas declarações de proteção de dados pelos autores do trabalho, de compromisso no tratamento ético e legal da informação recebida, em relação aos dados pessoais que possam ser entregues.

A organização deste capítulo é descrita de seguida. A primeira secção é o plano (4.1) descrevendo cada fase, seguindo-se o primeiro ataque (4.2), onde são detalhadas a implementação (4.2.2), os resultados (4.2.3) e a sua análise (4.2.4). Depois é explicada a campanha de consciencialização (4.3), isto é, quais os métodos usados para a realização da campanha. De seguida o segundo ataque (4.4), onde são detalhados a implementação (4.4.2), os resultados (4.4.3) e a análise (4.4.4), nesta

análise é feita a comparação dos resultados dos dois ataques. São ainda feitas outras considerações (4.5) e finalmente as conclusões (4.3.3).

4.1 Plano

O propósito deste projeto é a melhoria da consciencialização dos utilizadores para os ataques de *phishing* através de uma campanha de formação. Esta será antecedida de um ataque simulado, de modo a caracterizar o impacto nos vários grupos de utilizadores da comunidade académica que podem estar vulneráveis a este tipo de ataques. Posterior à campanha, haverá uma repetição do ataque, de modo a perceber quais os efeitos da campanha. Para tal, este caso de estudo foi dividido em três fases, cada uma com várias tarefas a cumprir:

Fase Um realização do primeiro ataque, onde, antes da sua execução, foram decididos quais os parâmetros a analisar nos resultados a obter, feita a definição da mensagem a ser enviada (detalhada em 4.2.2), preparação da ferramenta Gophish [3] para o lançamento do ataque (detalhada em 4.2.2 e o Anexo 5.1 apresenta as *interfaces*), realização do ataque e recolha dos dados, e, por fim, a sua apresentação e análise.

Fase Dois implementação da campanha de consciencialização, isto incluiu que após a análise dos resultados seja decidido que grupos seriam o público alvo para cada método de consciencialização, foi feita a seleção de informação relevante, aos membros da comunidade académica, para que possa ser exposta através dos vários métodos. Após completar estas tarefas foi dado início à campanha pondo em ação os vários métodos de consciencialização.

Fase Três realização do segundo ataque, que terá uma estrutura semelhante ao primeiro, e onde os parâmetros foram revistos, redefinida a nova mensagem a enviar, o ataque foi preparado e executado, e foi feita a recolha de dados e a sua análise.

Cada uma desta fases será, de seguida, detalhada, tendo atenção aos dados usados e recolhidos para destacar os principais resultados resultantes das várias ações.

4.2 Primeiro Ataque

O primeiro ataque de *phishing* decorreu entre 11 e 25 de novembro de 2021, onde foi enviado um *e-mail* falso, fazendo-se passar por um serviço de apoio da universidade, aos três grupos usando a plataforma Gophish. O conteúdo do *e-mail* incluía o texto para tentar enganar os utilizadores, e uma ligação que redirecionava a pessoa para uma página falsa, que pedia para inserir as credenciais.

Apesar do Gophish permitir a recolha de todos os campos da página falsa, neste projeto só o campo do utilizador foi recolhido, em altura nenhuma foi guardada alguma palavra-passe dos utilizadores que foram vítimas do ataque.

Os dados recolhidos foram analisados como preparação para a campanha de consciencialização.

4.2.1 Fase de Preparação

Antes da implementação do ataque tiveram de ser definidos alguns dos parâmetros para o ataque. Começando com a escolha da plataforma a ser usada, tendo o Gophish sido essa escolha devido a ser a ferramenta sugerida pelo Kit Metared, e ainda por ser usada em outros projetos

[3] https://getgophish.com/

semelhantes [24,42,43]. Foram feitos alguns testes para avaliar o desempenho da plataforma durante uma campanha.

De seguida foram definidas as datas para a execução do ataque, e também da campanha de consciencialização e do segundo ataque. No plano inicial o primeiro ataque ocorreria em novembro, a campanha em março e o segundo ataque em abril. A espera entre o primeiro ataque e a campanha deve-se a que o ataque das *pens* seria feito antes da campanha, em fevereiro.

Por fim foi decidido o conteúdo dos *e-mails*, sendo definido que a mensagem deveria incentivar a agir rapidamente, e que haveria uma ligação para uma página falsa onde fosse pedido para inserir as credenciais.

Após a definição destes três parâmetros, foi dado início à implementação.

4.2.2 Implementação

Neste capítulo para além da explicação de como foi executado o ataque é também apresentado como funciona uma campanha realizada através do Gophish.

Funcionamento de uma Campanha no Gophish

A plataforma Gophish é uma *framework open source* que permite a criação de *e-mails* e páginas falsas, a programação do envio de *e-mails* e a recolha de qualquer dado inserido caso a página falsa tenha um formulário com campos de texto. Todos estes recursos ajudam no lançamento de campanhas de *phishing*, onde podem ser enviadas centenas de mensagens de forma automática. O único fator externo necessário é um servidor SMTP, para gerir o envio dos *e-mails*. O processo de implementação de uma campanha com a plataforma Gophish está descrito na Figura 6.

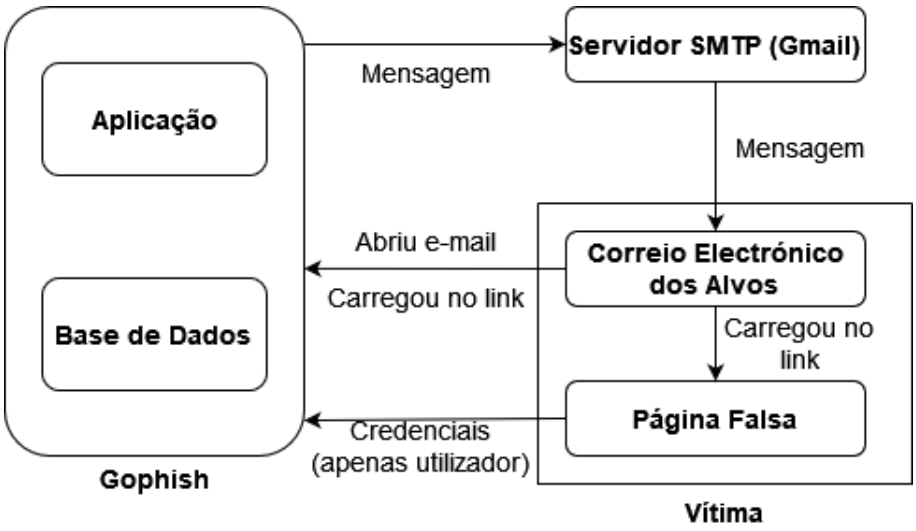

Figura 6: Diagrama do processo de uma campanha no Gophish.

Como visto na Figura 6 o Gophish é composto pela aplicação e pela base de dados, após definir todos os parâmetros necessários para uma campanha, de conectar uma conta de *e-mail* existente e de configurar um servidor SMTP, nesta campanha foi utilizado o do Gmail, pode ser dado início a uma campanha. A mensagem é enviada através do servidor SMTP a todos os alvos.

Após receber o *e-mail* a vítima do ataque pode fazer até três ações, abrir o *e-mail*, carregar na ligação e submeter credenciais. As ações realizadas ficam registadas na base de dados do Gophish, podendo ser acedidas na aplicação na secção de resultados.

A campanha de Gophish é apresentada em quatro passos na secção de resultados, estes são por ordem: *e-mail* enviado, *e-mail* aberto, carregar na ligação e submeter credenciais. Se um utilizador não interage de forma alguma com o *e-mail* só aparecerá *e-mail* enviado, caso contrario aparecerá o passo final do utilizador.

Execução da Campanha de Pishing

A aplicação do Gophish é acedida através de um *browser*, onde podemos encontrar a interface gráfica. Nesta é feita a criação das campanhas e a visualização dos resultados, todos os dados obtidos durante as campanhas são guardados na base de dados da plataforma (*SQLite*). Antes de iniciar cada campanha foram criados três grupos, inserindo o endereço de *e-mail*, o nome dos destinatários e o seu papel (serviço/faculdade/curso), também foi criado o modelo para os *e-mails* e para as páginas falsas. A criação da campanha foi feita selecionando o grupo, o modelo de *e-mail*, o modelo da página e o período em que os *e-mails* são enviados, isto determina o início da campanha. Terminar a campanha é feito de forma manual, não havendo limite de quanto tempo a campanha possa ficar ativa.

O modelo de *e-mail* criado, apresentado na Figura 7, foi semelhante para os três grupos, onde as diferenças foram, essencialmente, a ligação para o *site* que deveria ser acedido, na quinta e sexta linha, e o título para abordar cada grupo, presente na primeira linha.

```
1  Caro(a) Docente/Investigador,
2  Foi detectado um erro nos seus dados pessoais na plataforma SIDoc.
3  Recomendamos uma intervenção na sua conta o mais breve possível,
4  afim de evitar problemas na sua conta Docente/Investigador.
5  Aceda a sidoc.uma.pt para efectuar as mudanças necessárias:
6  sidoc.uma.pt

7  Cumprimentos,
8  Serviços de Apoio UMa
```

Figura 7: Modelo de *e-mail* enviado aos grupos na primeira campanha.

A abordagem utilizada na mensagem foi uma solicitação aos utilizadores para a verificação e a correção dos dados pessoais, e, de modo a incitar as pessoas a acederem às páginas, foi ainda incluído um sentido de urgência (Figura 7, linha 3). Na mesma figura, nas linhas 5 e 6, foram deixados as ligações para o acesso às páginas de autenticação, tendo o texto o endereço real, mas a ligação para o nosso servidor e para a página falseada.

As páginas às quais cada grupo foi direcionado foram cópias das páginas de *login* da página web o365.uma.pt (portal de acesso ao Office) para os funcionários, do SiDoc (Serviço de Informação dos

Docentes) para os docentes e investigadores e do InfoAlunos (Serviço de Informação dos Alunos) para os estudantes. Sendo a página uma cópia de páginas pré-existentes, o indicador que esta era falsa era o *URL*, que podia ser verificado ao passar o cursor por cima da ligação na mensagem, ou após abrir o *site* observando a barra de endereços.

Durante a criação das páginas foi selecionada a opção de recolher os dados submetidos nos formulários, tido sido recolhido apenas o campo do utilizador, realçando outra vez que não foi realizada a recolha do campo da palavra-passe.

Foi definido o endereço (http://orion.uma.pt/gophish) para aceder às páginas falsas criadas, embora o *URL* contenha o domínio 'uma.pt' (domínio da universidade), não foi disfarçada a parte 'gophish' com o objetivo de ser um indicador de que a página era falsa. Foi também criado um novo *e-mail*, Serviços de Apoio `<serv.de.apoio@gmail.com>`. O endereço criado aludia a um serviço de apoio pertencente à universidade, contudo foi escolhido um domínio externo à universidade (gmail.com) para que pudesse ser um indicador de uma mensagem fraudulenta.

Outro indicador é o cumprimento na primeira linha do corpo do e-mail, sendo usados termos gerais (Figura 7, linha 1), como Funcionário, Docente/Investigador e Estudante. Procurou-se não incluir em parte nenhuma da mensagem o nome do destinatário.

Para que o *e-mail* não fosse filtrado pelo servidor da universidade, foi pedido à UCI para colocar o endereço `<serv.de.apoio@gmail.com>` na *white list*, desta forma era garantido a mensagem chegar às caixas de correio de todos os utilizadores, sem ser filtrada ou enviada para a pasta de Lixo do Outlook.

As campanhas dos funcionários e docentes/investigadores tiveram a duração de quinze dias. Os *e-mails* foram enviados em poucas horas devido a serem grupos de poucas centenas de utilizadores.

Já a campanha dos estudantes teve duração de 17 dias e tal deveu-se a uma falha no envio inicial no Gmail, sendo necessário terminá-la depois de um dia e iniciar uma segunda para reenviar alguns dos *e-mails* que falharam, e enviar os restantes em falta. Este envio durou vários dias devido a limites máximos diários de envio do servidor Gmail.

Para iniciar a análise desta campanha, a Figura 8 mostra o número de pessoas que abriram o *e-mail* em cada dia da duração das campanhas, tenham ou não feito os passos seguintes.

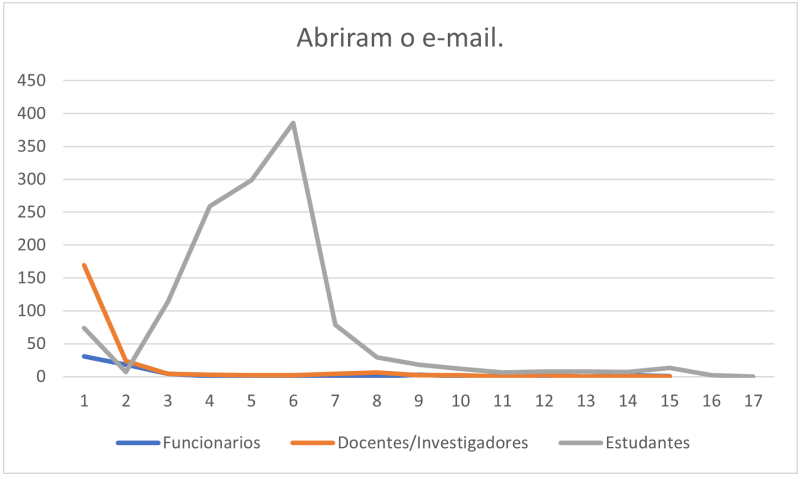

Figura 8: Número por dia de quem abriu o *e-mail* na primeira campanha.

Por análise à Figura 8, podemos observar que a maior parte dos membros de cada grupo interage com o *e-mail* assim que o recebe, visto que para os funcionários e docentes/investigadores os *e-mails* foram abertos em apenas algumas horas, todos no mesmo dia, ou seja, o primeiro dia da campanha foi quando mais pessoas abriram o *e-mail*. Em relação aos estudantes, o primeiro dia da segunda campanha correspondem ao terceiro dia do gráfico, e o envio dos *e-mails* foi feito ao longo de quatro dias, logo o primeiro dia corresponde apenas aos estudantes da primeira campanha, no segundo dia não houve envio de *e-mails*, e os dias em que mais *e-mails* foram abertos foram o quarto, quinto e sexto dia em que o maior número de *e-mails* foram enviados.

4.2.3 Resultados

Neste capítulo serão apresentados os resultados da campanha, começando com os resultados globais, seguidos dos resultados de cada grupos. A apresentação dos resultados dos grupos será feita pela seguinte ordem: funcionários, docentes/investigadores e, por fim, os estudantes.

Os dados recolhidos pelo Gophish são apresentados em quatro passos, sendo esta a ordem dos acontecimentos:

1. envio do *e-mail* pelo SMTP do Gmail:
2. abertura do *e-mail* (notificação ao Gophish);
3. carregar na ligação no *e-mail* (encaminhamento para a página falsa do Gophish);
4. submeter credenciais (cópia de página de login).

Assim, se alguém submeteu as credenciais, implica ter feitos os outros passos todos e o mesmo aplica-se aos passos restantes. Os resultados de cada passo são apresentados em três linhas:

- frequência absoluta, ou seja, dados absolutos;
- frequência relativa (%), ou seja a percentagem sobre a frequência absoluta;
- frequência relativa (%) em relação ao passo anterior;

Isto é, credenciais enviadas em relação a carregaram na ligação, carregaram na ligação em relação a *e-mails* abertos, e neste caso *e-mails* abertos em relação aos *e-mails* enviados mantém o mesmo valor que da frequência relativa (%).

Tabela 1: Resultados globais da primeira campanha.

E-mails enviados	**E-mails Abertos**	**Carregaram na Ligação**	**Credenciais Enviadas**
4431	1605	1031	697
-	36,22%	23,27%	15,73%
-	-	64,24%	67,60%

Resultados Globais

No decorrer das três campanhas do primeiro ataque foram obtidos os seguintes resultados (presentes na Tabela 1): *e-mails* enviados foram 4431, os *e-mails* abertos foram 1605, resultando numa taxa de 36,22% em relação aos emails enviados; os utilizadores que carregaram na ligação foram 1031, resultando em 23,27% de utilizadores nesta situação, mas 64,24% de utilizadores em

relação aos que abriram o *e-mail*; e, as credenciais submetidas foram 697, 15,73% do total dos utilizadores, mas 67,6% dos utilizadores que já tinham carregado na ligação.

Resultados de Funcionários

Os resultados para cada grupo foram os seguintes, começando com os funcionários (presentes na Tabela 2): *e-mails* enviados 211, *e-mails* abertos 63 (27,91%), carregaram na ligação 32 (14,88%), credenciais enviadas 19 (8,84%). A última linha da Tabela 1 frequência em relação ao passo anterior, carregaram na ligação 53,33% e credenciais enviadas 59,38%.

Tabela 2: Resultados dos funcionários da primeira campanha.

E-mails enviados	E-mails Abertos	Carregaram na Ligação	Credenciais Enviadas
215	60	32	19
-	27,91%	14,88%	8,84%
-	-	53,33%	59,38%

Resultados de Docentes/Investigadores

Os resultados do grupo de docentes/investigadores (presentes na Tabela 3) foram: *e-mails* enviados 598, *e-mails* abertos 221 (37,71%), carregaram na ligação 114 (19,19%), e enviaram credenciais 69 (11,62%). A última linha da Tabela 3 frequência em relação ao passo anterior, carregaram na ligação 53,33% e credenciais enviadas 59,38%.

Tabela 3: Resultados dos docentes/investigadores da primeira campanha.

E-mails enviados	E-mails Abertos	Carregaram na Ligação	Credenciais Enviadas
594	224	114	69
-	37,71%	19,19%	11,62%
-	-	50,89%	60,53%

Resultados de Estudantes

O grupo de estudantes obteve os seguintes resultados (presentes na Tabela 4): *e-mails* enviados 3622, *e-mails* abertos 1321 (36,47%), carregaram na ligação 885 (24,43%), e enviaram credenciais 609 (16,81%). A última linha da Tabela 4 frequência em relação ao passo anterior, carregaram na ligação 66,99% e credenciais enviadas 68,81%.

Tabela 4: Resultados dos estudantes da primeira campanha.

E-mails enviados	E-mails Abertos	Carregaram na Ligação	Credenciais Enviadas
3622	1321	885	609
-	36,47%	24,43%	16,81%
-	-	66,99%	68,81%

Apesar de terem sido feitas duas campanhas para os estudantes, foi decidido considerar os resultados da primeira campanha em conjunto com os resultados da segunda campanha. Embora a segunda campanha tenha tido uma duração menor, uma grande parte (61%) dos estudantes da Faculdade de Ciências da Vida encontravam-se neste grupo, e as percentagens obtidas na primeira campanha não tem uma grande diferença da segunda campanha.

Outros Resultados

Foram pedidos dados extras à UCI sobre pedidos de ajuda/esclarecimento ou alertas sobre o ataque. Em relação aos funcionários: 3 pediram ajuda/esclarecimento por *e-mail* e 14 pediram por telefone e de forma presencial, ainda 8 funcionários alertaram que tinham recebido e sabiam que o *e-mail* era *phishing*. Entre os docentes/investigadores: 13 pediram ajuda/esclarecimento por *e-mail*, 9 por telefone e de forma presencial e 5 pela Ferramenta de Suporte (através de *tickets*), 6 alertaram saber que tinham recebido e sabiam que o *e-mail* era *phishing*. Já os estudantes: 8 pediram ajuda/esclarecimento por *e-mail* e 2 alertaram que tinham recebido e sabiam que o *e-mail* era *phishing*.

Para além das pessoas que contactaram diretamente os serviços oficiais da universidade, houveram 88 respostas ao *e-mail* usado no ataque. Houve 2 respostas de funcionários a dizer que atualizaram os dados. Para os docentes/investigadores 9 pediram para esclarecer quais dados estavam errados, 3 avisaram que não tinham acesso à conta, 2 respostas sobre terem atualizados os dados, 1 desconfiou ser um *e-mail* de *phishing* e 1 sabia que era um ataque de *phishing*. Em relação aos estudantes 53 pediram para esclarecer quais dados estavam errados, 2 avisaram que não tinham acesso à conta, 12 responderam que atualizaram os dados, 1 desconfiou ser um *e-mail* de *phishing* e 2 sabiam que era um ataque de *phishing*.

Em relação ao acesso às caixas de correio é necessário ter em conta duas situações, aqueles que não acederam durante o decorrer da campanha e aqueles que reencaminham as mensagens da caixa da universidade para outra caixa. Entre os funcionários 23 não acederam à caixa durante a campanha e 3 reencaminharam. Para os docentes/investigadores 134 não acederam à caixa e 57 reencaminharam. Já os estudantes 445 não acederam à caixa, 109 reencaminharam as mensagens. Em todas estas situações, o número de pessoas que, potencialmente ficaram fora desta ação foi baixo.

4.2.4 Análise

A análise dos resultados para este primeiro ataque é uma primeira avaliação do comportamento dos membros da comunidade académica, servindo para determinar se há necessidade de educá-los para o tema da Engenharia Social. Começou por ser feita a comparação entre os três grupos e, dentro de cada grupo, a comparação entre os serviços para os funcionários, entre as faculdades e laboratórios para os docentes/investigadores, e entre as faculdades/escolas, os ciclos e os anos para os estudantes.

Embora também seja analisada a frequência relativa (%) na comparação entre grupos, é dada maior importância aos dados da frequência relativa (%) em relação ao passo anterior, isto porque desta forma são avaliados a partir do segundo passo de abrir o *e-mail*. Esta decisão foi tomada pois existem vários fatores que levam a que as pessoas não abram os seus *e-mails*, como não aceder à sua conta regularmente, só prestar atenção a *e-mails* de remetentes específicos e definir as suas próprias regras de filtragem de *e-mails* recebidos.

Esta abordagem de análise garante perceber se as pessoas que abriram o *e-mail* e não carregaram na ligação, foram capazes de identificar pelo menos um dos indicadores que o *e-mail* não foi enviado por um serviço da universidade e que era falso. E ainda os que carregaram na ligação mas não enviaram as credenciais foram capazes de identificar que a página não era oficial.

Análise Global

Começando por comparar a frequência relativa (%) entre os três grupos e os resultados globais é obtido o seguinte gráfico da Figura 9. O Total Global é obtido ao somar os valores absolutos de cada grupo, e calcular as frequências relativas (%) a partir desses valores, não é feita a média entre os três grupos. Este valor estará sempre mais aproximado ao valor do grupo estudantes, visto este ser o grupo com mais elementos, têm mais influência no resultado global.

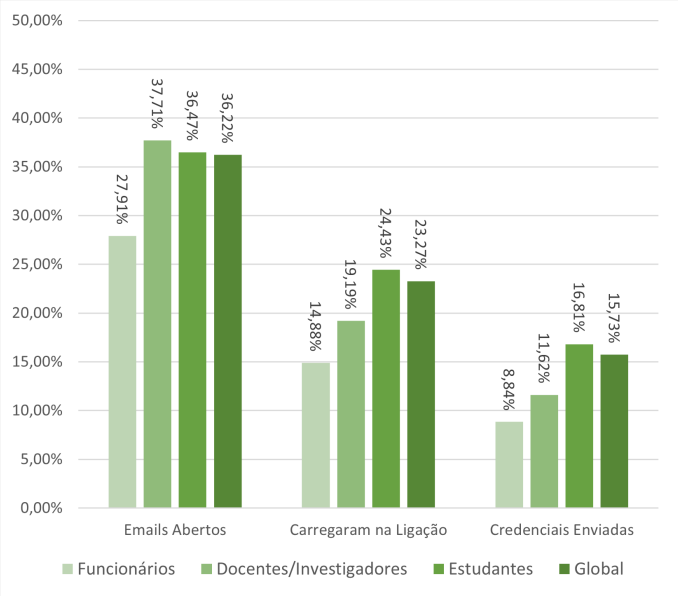

Figura 9: Comparação da frequência relativa (%) dos grupos e do total global da primeira campanha, por passo.

O grupo com menores valores de frequência relativa (%) em todos os passos são os funcionários, isto era esperado, não só por ser o grupo mais pequeno, como também por serem os utilizadores com o maior conhecimento dos serviços reais da universidade e ainda haver a possibilidade de que em alguns serviços o uso do *e-mail* não seja tão proeminente quanto outros.

Entre os os docentes/investigadores e os estudantes, os docentes/investigadores foram os com mais frequência de *e-mails* abertos, enquanto os estudantes têm as maiores frequências nos passos carregaram na ligação e credenciais enviadas, mais uma vez estes resultados eram esperados, pois foi previsto os estudantes serem o grupo com maior dificuldade a identificar um *e-mail* falso vindo da universidade.

Esta dificuldade é ainda melhor observada ao olhar para o gráfico da Figura 10, que mostra a frequência relativa (%) em relação ao passo anterior. Isto é, dos estudantes que abriram o *e-mail*, 66,99% carregaram na ligação, que em si já é perigoso por poder haver *download* de ficheiros maliciosos. Ainda daqueles que carregaram na ligação, 68,81% enviaram as credenciais, já referido

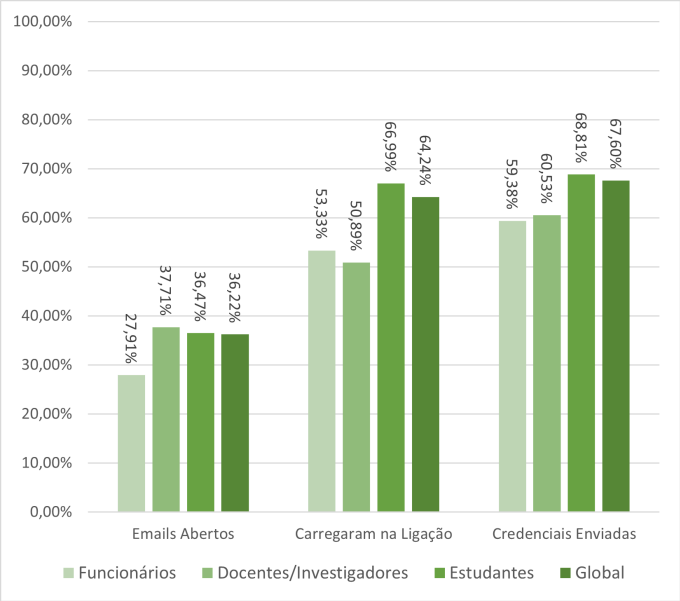

Figura 10: Comparação da frequência relativa (%) em relação ao passo anterior, dos grupos e do global da primeira campanha.

e observado na Tabela 4, isto equivale a 609 estudantes que podiam ter expostos os seus dados pessoais.

Entre os grupos de funcionários e docentes/investigadores, não houve muita discrepância nas frequências relativas (%) em relação ao passo anterior, para os que abriram o *e-mail* 53,33% e 50,89% carregaram na ligação, respetivamente, sendo uma diferença de 2,44% entre os grupos. E dos que carregaram na ligação 59,38% e 60,53% enviaram credenciais, respetivamente. Isto significa que 19 funcionários (Tabela 2) e 69 docentes/investigadores (Tabela 3), não só podiam ter exposto os seus dados pessoais, como qualquer outra informação a que tenham acesso devido aos seus cargos.

Esta comparação permitiu concluir que neste primeiro ataque o grupo de estudantes é o mais vulnerável, sendo o grupo com mais dificuldade em reconhecer um *e-mail* falso e mais dificuldade em identificar um *site* falso. Nos três grupos podemos considerar que mais de metade das pessoas que abrem o *e-mail* não o identificam como falso, e também mais de metade que carrega na ligação não identifica a página como falsa, podendo isto acontecer por falta de atenção ou falta de conhecimentos. Durante a criação das páginas foi selecionada a opção de recolher os dados submetidos nos formulários, tido sido recolhido apenas o campo do utilizador, realçando outra vez que não foi realizada a recolha do campo da palavra-passe.

De seguida é feita a comparação dentro de cada grupo, para os funcionários são comparados cada serviço, para docentes/investigadores são comparadas as faculdades e laboratórios, e para os estudantes é comparado faculdades/escolas, ciclos e anos. Vai ser usada a frequência relativa (%) em relação ao passo anterior para o resto da análise.

Não são revelados os nomes dos serviços e das faculdades e laboratórios no caso dos funcionários e docentes/investigadores. E ainda, devido a que alguns serviços, faculdades/escolas e laboratórios têm uma amostra pequena, e que ciclos e anos não estão definidos para alguns estudantes, foi criado

a categoria outros. Nesta categoria foram incluídos todos os serviços, faculdades e laboratórios com menos de dez pessoas, e os alunos com ciclos e anos não definidos.

Análise de Funcionários

Os funcionários estão divididos em quatro serviços mais a categoria de outros. Esta categoria incluí vinte e oito serviços, em que o número de pessoas pertencentes é inferior a dez. Os serviços são representados por letras, e o número de membros está representado na Tabela 5 pela mesma ordem que no gráfico da Figura 11.

Tabela 5: Número de funcionários por serviço.

Serviços	Número de Funcionários
Serviço A	50
Serviço B	17
Serviço C	11
Serviço D	11
Outros Serviços	126

No gráfico da Figura 11 é possível observar que o Serviço A é o mais vulnerável a ataques, tendo a maior frequência relativa (%) no segundo passo com 71,43% que equivale a 10 pessoas, e, mesmo não tendo a maior frequência para o último passo, é o segundo valor mais alto com 70,00% que equivale a 7 pessoas, junto ao facto que é o serviço de maior dimensão, mostra ser o mais propício a comportamentos de risco.

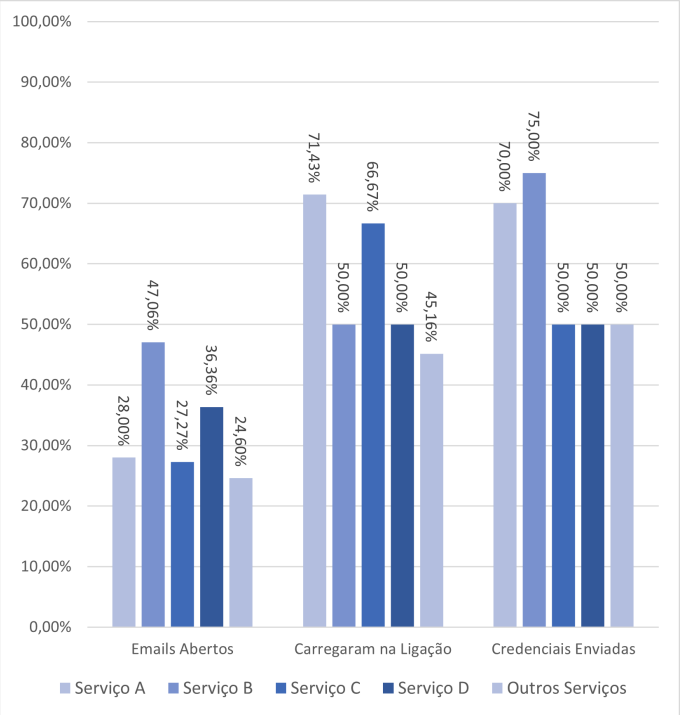

Figura 11: Comparação da frequência relativa (%) em relação ao passo anterior dos funcionários da primeira campanha.

De seguida o Serviço C destaca-se no passo carregaram na ligação com 66,67% com o segundo maior valor, mas apenas equivale a 2 pessoas. No passo credenciais enviadas o Serviço B tem a maior frequência com 75,00%, que equivale a 3 pessoas apenas. É de salientar que os resultados mostram que no geral os funcionários não conseguiram identificar o *e-mail* e a página como falsos, sendo isto confirmado com o gráfico da Figura 11, pois nos últimos dois passos os valores são de 50,00% ou mais, com a exceção do passo carregaram na ligação para os Outros serviços com 45,16% que equivale a 14 pessoas.

Apesar de o Serviço A ter sido identificado como o mais vulnerável, é de notar que os restantes serviços têm amostras mais pequenas, e que os Outros Serviços são um conjunto de vinte e oito, onde alguns são constituídos por uma só pessoa. Esta diferença na dimensão pode fazer com que a análise das comparações não seja adequada, pois o número de membros em cada serviço não é de relevo.

Análise de Docentes/Investigadores

O grupo dos docentes/investigadores não é tão afetado pelo problema da dimensão da amostra quanto os funcionários. Com seis faculdades, dois laboratórios e a categoria de Outros Laboratórios, conjunto de dez laboratórios constituídos por menos de dez pessoas, os tamanhos da amostra de cada faculdade e laboratório são mais relevantes, mesmo havendo diferenças significativas entre o número de membros de cada.

Por ordem, tal qual está no gráfico da Figura 12, o número de membros das faculdade e laboratórios está representado na Tabela 6.

Tabela 6: Número de docentes/investigadores por faculdade e laboratório.

Faculdades/Laboratórios	Número de Docentes/Investigadores
Faculdade A	149
Faculdade B	110
Faculdade C	84
Faculdade D	68
Faculdade E	51
Faculdade F	35
Laboratório A	53
Laboratório B	21
Outros Laboratórios	23

No passo carregaram na ligação a Faculdade F destaca-se com 91,67%, que significa que das 12 pessoas que abriram o *e-mail*, 11 carregaram na ligação.

No último passo duas faculdades sobressaem em relação às restantes, a Faculdade E teve 100% das pessoas que carregaram na ligação também enviaram credenciais, mas apenas corresponde a 3 membros. Devido a que a frequência nos passos anteriores é baixa, conseguindo ser a mais baixa entre o grupo, com 21,57% e 27,27%, por ordem de ações, o valor absoluto final não alto.

Já a Faculdade F, em que 11 membros tinham carregado na ligação, este valor de 90,91% significa que 10 membros enviaram credenciais. Entre faculdades e laboratórios esta é a faculdade mais vulnerável, com valores de frequência elevados para prosseguir para o próximo passo.

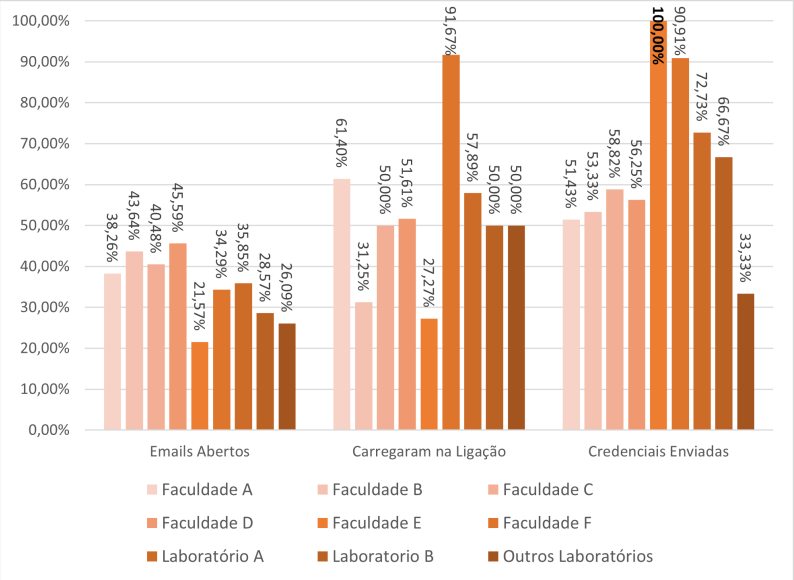

Figura 12: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e laboratórios dos docentes/investigadores da primeira campanha.

No entanto, da mesma forma que foi observado no grupo dos funcionários, e com algumas exceções, no geral os docentes/investigadores não conseguiram identificar o *e-mail* e a página como falsos, observando novamente o gráfico da Figura 12, em ambos os passos os valores da frequência são de 50,00% ou mais.

Após a análise de ambos os grupos de funcionários e docentes/investigadores foi possível responder às questões de qual serviço e faculdade/laboratório eram os mais vulneráveis. Também foi confirmada a necessidade de proceder com a campanha de consciencialização pois ambos apresentam tendência a comportamentos de risco, com especial atenção a estes grupos por serem aqueles com acesso a mais informação, pessoal e outros dados relativos à universidade.

Análise de Estudantes

O último grupo a analisar foram os estudantes, onde os parâmetros comparados são as faculdades, os ciclos e os anos, para este grupo as faculdades/escolas são reveladas.

Os cursos profissionais (CTeSP) são considerados em conjunto com as faculdades/escolas, são considerados como um ciclo próprio quando comparados com o 1º ciclo (licenciatura), 2º ciclo (mestrado) e 3º ciclo (doutoramento), e também por serem um ciclo diferente os anos de curso são a sua própria categoria.

A categoria Outros em cada indicador são para estudantes que ou estão inscritos como externos em diversas cadeiras não específicas de um só curso, ou são estudantes de um curso para um determinada língua (por exemplo: Curso de Português Língua Não Materna), e por isso não tem faculdade, ciclo ou ano definidos.

Por fim o 1º ciclo 3º ano (Figura 15) inclui todos os estudantes com três ou mais matriculas na universidade , e o 1º ciclo 4º ano (Figura 15) representa o quarto ano de enfermagem, sendo o único curso com mais de três anos de duração.

Começando com a comparação entre faculdades, o número de membros de cada faculdade por ordem do que é apresentado no gráfico da Figura 13 está representado na Tabela 7.

Tabela 7: Número de estudantes por faculdade e escola.

Faculdades/Escolas	Número de Estudantes
CTeSP	564
Faculdade de Artes e Humanidades	868
Faculdade de Ciencias Exatas e da Engenharia	722
Faculdade de Ciencias Sociais	909
Faculdade de Ciências da Vida	171
Escola Superior de Tecnologias e Gestão	160
Escola Superior de Saúde	153
Outros	93

Ao observar os resultados do gráfico 13, nenhuma faculdade destaca-se como a que melhor reconheceu os indicadores do *e-mail* ser falso, fazendo com que os estudantes carregassem na ligação. A FCEE destaca-se por ter o valor mais baixo com 57,55%, equivalente a 183 estudantes, no entanto o valor não é baixo o suficiente para afirmar que esta faculdade tenha menos comportamentos de risco.

Para aqueles que enviaram as credenciais, por não se aperceberem que tinha sido redirecionados a uma página falsa, também não se destacada nenhuma faculdade como a mais inclinada para esta ação, mais uma vez os valores da frequência são semelhantes. A categoria de Outros destaca-se com o valor mais baixo de 50,00%, mas devido a que no passo de abrir o *e-mail* houve pouca adesão, apenas 6, esta percentagem equivale a apenas 2 dos 4 estudantes que carregaram na ligação, é um valor baixo para uma análise adequada.

Estes resultados demonstram que nenhuma faculdade têm maior tendência a ser vítima de *phishing* que outras, mas com a maioria dos resultados entre os 60% e os 80%, demonstra que em todas as faculdades existem alunos com falta de conhecimentos sobre como reconhecer *e-mails* e páginas falsas.

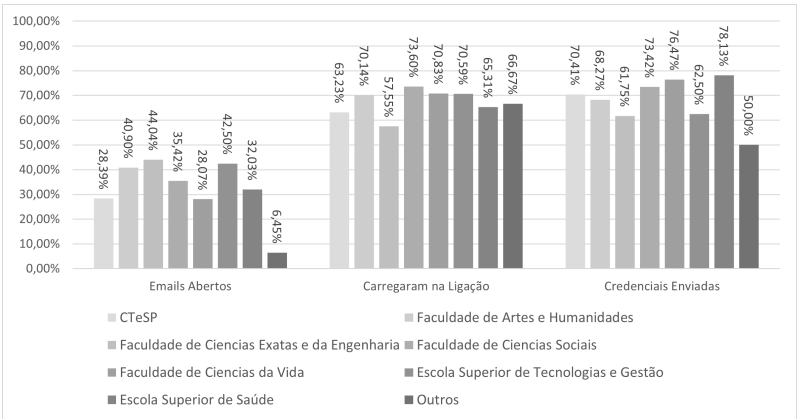

Figura 13: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e escolas dos estudantes da primeira campanha.

A próxima análise são os ciclos, pela ordem do gráfico da Figura 14, são apresentados o número de estudantes na Tabela 8. Para esta análise, embora 1º ciclo e CTeSP sejam considerados ciclos diferentes, são equiparáveis em termos de matrículas, enquanto a categoria outros não é possível fazer essa distinção.

Tabela 8: Número de estudantes por ciclo.

Ciclo	Número de Estudantes
1º Ciclo	2462
2º Ciclo	434
3º Ciclo	63
CTeSP	546
Outros	117

Ao examinar o gráfico 14 o 1º ciclo foi o que mais estudantes carregaram na ligação, com 69,70%, e o 3º ciclo o que menos estudantes carregaram, com 47,06%, estes valores equivalem a 671 e a 8 estudantes, respetivamente. No entanto é percetível que os ciclos com estudantes mais antigos, têm tendência a apresentar valores mais baixos.

No passo credenciais enviadas, o segundo ciclo apresenta valores mais baixos que o 1º ciclo e CTeSP, enquanto o 3º ciclo tem o valor mais alto. Tendo o 3º ciclo uma amostra menor isto é esperado, pois os 87,50% equivale a 7 estudantes dos 8 que carregaram na ligação.

Mais uma vez é verificado que com amostras mais baixas, há maior tendência para que a frequência do passo final tenha um valor mais alto, que acontece com o 3º ciclo no passo de credenciais enviadas.

No geral, entre os ciclos dos estudantes, é percetível que os estudantes de ciclos mais baixos têm mais tendência a comportamentos de risco perante *e-mails* e páginas que se fazem passar por serviços da universidade.

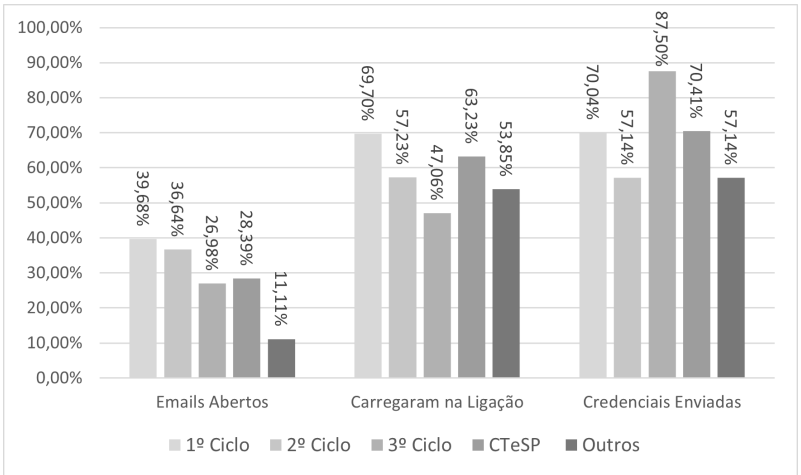

Figura 14: Comparação da frequência relativa (%) em relação ao passo anterior dos ciclos dos estudantes da primeira campanha.

Por fim vamos analisar os estudantes por ano, este indicador volta a ter a dificuldade de analisar algumas categorias em que o número da amostra é demasiado pequeno, pode ser observado na Tabela 9, como acontece com o 3º ciclo 2º ano, PLE, os Pos-Grad (B) e Outros, todos estes têm menos de trinta elementos. Para PLE e Outros não houveram alunos a abrir o *e-mail*, e para 3º ciclo 2º ano só 1 estudante abriu o *e-mail*.

Tabela 9: Número de estudantes por ano.

Ciclo e Ano	Número de Estudantes
1º Ciclo 1º Ano	1000
1º Ciclo 2º Ano	685
1º Ciclo 3º Ano	746
1º Ciclo 4º Ano	29
2º Ciclo 1º Ano	197
2º Ciclo 2º Ano	237
3º Ciclo 1º Ano	53
3º Ciclo 2º Ano	9
CTeSP 1º ano	288
CTeSP 2º ano	258
Inf. 60 ECTS	71
PLE	22
Pos-Grad (B)	24
Outros	3

Para os demais anos, é considerado para a maior parte dos estudantes que a primeira matrícula numa instituição de ensino superior são o primeiro ano do 1º ciclo, dos CTeSP e dos Inf. 60 ECTS.

Tendo em conta o tempo de inscrição, podemos notar através do gráfico da Figura 15 que, o primeiro ano de cada ciclo e dos CTeSP são os que mais carregam na ligação em comparação com os outros anos do mesmo ciclo.

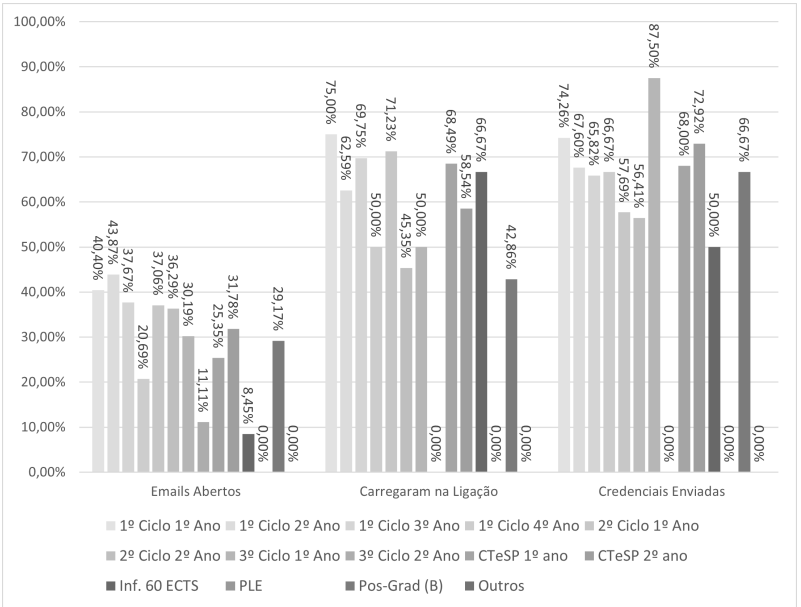

Figura 15: Comparação da frequência relativa (%) em relação ao passo anterior dos anos dos estudantes da primeira campanha.

No último passo, submeter credenciais, mantêm-se o mesmo padrão com a exceção dos CTeSP, em que o 2º ano teve um percentagem maior de pessoas a submeter credenciais em comparação com o 1º ano.

No geral quanto menor o tempo de inscrição maior a tendência de haver comportamentos de risco. No entanto em alguns casos não é possível fazer análise por ano, porque ou a amostra já é pequena, ou há pouca adesão no passo de abrir o *e-mail*.

Ambas as análises dos ciclos e dos anos mostra que existe diferença no comportamento de estudantes mais antigos em relação aos mais novos. Isto significa que para o grupo dos estudantes a área de estudo não afeta a sua perceção de um *e-mail* falso, mas a idade e/ou anos em que pertencem à instituição, já pode influenciar.

Conclusões da Análise

Em conjunto com os resultados dos funcionários e dos docentes/investigadores, pode ser concluído que os resultados de grupos pequenos não são adequados a analisar, pois muitas vezes os valores observados não correspondem aos grupos restantes. enquanto os valores dos grupos com maior número de elementos são próximos ou mais comparáveis entre si, e ainda em alguns casos não existem valores para analisar nos grupos pequenos. Em grupos mais pequenos uma frequência mais alta não é equivalente a um número alto de pessoas que são vulneráveis aos ataques, às vezes corresponde a uma ou duas pessoas, e pode induzir em erro aquando da análise dos gráficos.

Este tipo de dificuldades na análise dos resultados também podem ser observado em grupos com uma amostra considerável, mas onde não houve adesão na abertura do *e-mail*. E como referido anteriormente, estes resultados estão a ser analisados a partir desse passo, por haver variados fatores não relacionados com a identificação de indicadores de *e-mails* e páginas falsas, que causam uma pessoa a não abrir um *e-mail*.

No entanto, de forma geral, é verificada a necessidade de realizar a campanha de consciencialização, por ter sido notado que um grande número de membros da comunidade académica da universidade, após lerem o *e-mail* e acederem à página, não são capazes de identificar os sinais que indicam que estes não são válidos.

Com a análise dos resultados, foi decidido que os *e-mails* informativos seriam enviados para todos os grupos, mas limitado às pessoas que carregaram na ligação e enviaram credenciais. Esta decisão deve-se ao facto de que ambas as ações são de risco, e as pessoas que as executam estão a por em perigo os seus dados e os dados de outros.

Também foi decidido que a sessão de formação presencial seria disponibilizada para os grupos de funcionários e docentes/investigadores, limitada às pessoas que enviaram as credenciais. Esta limitação deve ao facto que submeter credenciais é a ação mais perigosa, pois dá acesso à conta e aos dados da pessoa, como tal as pessoas que a realizaram precisam de formação extra. Não será disponibilizada aos estudantes, pois estes são um grupo maior e as sessões funcionam melhor em grupos de menores dimensões, e também não é possível realizar sessões suficientes para todos os estudantes em grupos menores.

4.3 Campanha de Consciencialização

A campanha de consciencialização, seguida de um primeiro ataque, faz parte da abordagem de treino integrado, significa isto que após a análise dos resultados começou a difusão da informação

através dos diferentes métodos escolhidos consoante os resultados de cada grupo. Estes métodos foram afixação de cartazes, envio de *e-mails* informativos e sessão de formação presencial. Outro formato para divulgar a informação, usado durante o segundo ataque de *phishing* e durante o ataque via *pens*, quando é feito o redirecionamento após carregar na ligação ou após abrir um ficheiro, é a abertura de uma página web com uma chamada de atenção a possíveis ataques e com alguma informação sobre o tipo de ataque.

Após terminar o período do primeiro ataque de *phishing* (11 a 25 de novembro) foi enviado um *e-mail* de alerta a 2 de dezembro, a todos os membros da universidade, a explicar que o ataque fazia parte da campanha de consciencialização que a universidade estava a realizar e que o ataque era falso. Para além de servir para assegurar as pessoas que nenhum dado pessoal tinha sido roubado, também serviu para alertar as pessoas que estão vulneráveis a este tipo de ataques. O objetivo deste alerta era incentivar a que os membros dos grupos tivessem interesse em aprender sobre a Engenharia Social, mais especificamente sobre *phishing*.

De seguida, os cartazes foram afixados nos placares da universidade com o intuito de chamar a atenção sobre a campanha. Não continham informação sobre Cibersegurança ou Engenharia Social e, tal como o *e-mail* de alerta, o objetivo era incentivar os membros da universidade a aprender sobre esses temas.

4.3.1 *E-mail informativo*

O *e-mail* informativo foi enviado a 20 de maio, aos três grupos, mas apenas às pessoas que carregaram na ligação e submeteram credenciais no ataque simulado. Foi decidido que quem abriu o *e-mail* seria contabilizado até o dia anterior ao início do segundo ataque, dando assim o máximo de tempo possível para consultar o *e-mail* e os recursos disponibilizados. Para os funcionários e docentes/investigadores foi contabilizado durante três semanas, e para os estudantes foi contabilizado durante uma semana.

O *e-mail* consistia na explicação da campanha e uma ligação para descarregar uma apresentação sobre ataques de *phishing*, incluindo esta algumas dicas para identificar *e-mails* fraudulentos. No *e-mail* informativo também foi disponibilizada a ligação para a plataforma NAU[4], pois esta fornece cursos de curta duração sobre várias áreas da Cibersegurança para além do *phishing*. Estes cursos foram desenvolvidos por algumas universidades portuguesas e pela MetaRed. Por fim, foi explicado o procedimento a seguir em caso de dúvida ou deteção de um ataque, que passa por contactar os responsáveis de informática e segurança através do endereço de *e-mail* facultado.

Este *e-mail* foi enviado a um total de 1031 pessoas (Tabela 10, linha 1), divididos da seguinte forma: 32 funcionários, 114 docentes/investigadores e 885 estudantes. O *e-mail* foi enviado através da plataforma Gophish para ser possível termos algum retorno sobre a quantidade de mensagens lidas.

Os funcionários foram o grupo com menor adesão à consulta do *e-mail* (Tabela 10, linha 2), onde das 32 pessoas ao qual foi enviado, 15 (46,88%) abriram, não sendo possível verificar quantas transferiram a apresentação, nem quantas acederam à página da NAU.

Os docentes/investigadores foram os que mais aderiram à consulta do *e-mail* (Tabela 10, linha 3), em que das 114 pessoas ao qual foi enviado, 64 (56,14%) abriram a mensagem, mais uma vez não sendo possível verificar os dados em relação à apresentação e à página fornecida.

[4]https://www.nau.edu.pt/pt/

Tabela 10: Resultados do envio do *e-mail* informativo.

Grupo	*E-mails* Enviados	*E-mails* Abertos	Frequência Relativa (%)
Global	1031	540	52,37%
Funcionários	32	15	46,88%
Docentes/Investigadores	114	64	56,14%
Estudantes	885	461	52,09%

Por último, para o grupo dos estudantes (Tabela 10, linha 4), dos 885 *e-mails* enviados, 461 (52,09%) foram abertos, não há dados em relação à apresentação e à página fornecida.

Nos três grupos apenas metade dos membros abriram o *e-mail*, o que não garante que tenham consultado os recursos disponibilizados para se educarem sobre Cibersegurança. De qualquer forma, estes dados foram recolhidos para, após a segunda campanha, verificar se o *e-mail* informativo teve algum impacto na perceção das pessoas sobre o que são *e-mails* fraudulentos, e se este método de consciencialização é efetivo.

4.3.2 Sessão de Formação

O método seguinte da campanha de consciencialização foi a sessão de formação presencial, disponibilizada aos funcionários e docentes/investigadores que submeteram as credenciais durante o primeiro ataque. Sendo o universo de utilizadores bastante grande, foi necessário reduzir e considerou-se que este grupo dos funcionários e docentes/investigadores era um grupo suficientemente alargado para realizar a formação.

Assim, foi enviado um *e-mail* a 88 pessoas, 19 funcionários e 69 docentes/investigadores, a convidá-las a assistir à sessão de formação e pedindo ainda a confirmação da sua presença. Apesar de algumas pessoas mostrarem interesse, no dia da formação apenas 2 pessoas estiveram presentes.

Durante a sessão de formação, a apresentação consistiu numa identificação dos ataques de *phishing*, algumas dicas para a deteção de *e-mails* fraudulentos, exemplos de *e-mails* falsos e outros cuidados a ter na utilização de correio eletrónico de forma a prevenir comportamentos de risco. Ainda, durante a sessão, foram partilhadas experiências de ataques onde as pessoas presentes foram alvos e foram esclarecidas dúvidas em relação aos procedimentos a tomar nestes casos.

Para as pessoas convidadas que não assistiram à sessão foi enviado outro *e-mail* com uma ligação para descarregarem a apresentação *powerpoint* usada durante a sessão, foi relembrado que podiam aceder ao *site* da NAU onde encontram mais formações sobre Cibersegurança, e qual é o procedimento a seguir em caso de dúvida ou deteção de um ataque.

Por fim, já fazendo parte dos ataques, as páginas para quais as pessoas foram redirecionadas no ataque via *pens USB* e no segundo ataque de *phishing* eram páginas de alerta, que explicavam o objetivo dos ataques e que estes eram falsos. enquanto a página do ataque de *pens* (Anexo 5.1 Figura 79) servia como chamada de atenção, sem expor muita informação, a página do segundo ataque de *phishing* (Anexo 5.1Figura 80 e Figura 81) continha algumas dicas para identificar *e-mails* fraudulentos e explicava que o procedimento a seguir em caso de duvida ou deteção de uma ataque era contactar os responsáveis de informática e segurança através do endereço de *e-mail* facultado.

4.3.3 Conclusões

Todos os métodos previstos para a campanha de consciencialização foram aplicados, no entanto o *e-mail* informativo e a sessão de formação decorreram mais tarde do esperado. Inicialmente, tanto o *e-mail* como a sessão, estavam planeados para ocorrerem entre dois a três meses após o primeiro ataque (dando tempo para ocorrer o ataque via *pens*), tal não foi possível devido a fatores externos a este projeto. O tempo decorrido pode ter causado a falta de interesse pois o ataque já não estaria presente na memória dos membros da universidade.

Era esperado haver mais adesão à sessão de formação, mas mais uma vez tendo em conta o tempo que passou entre o primeiro ataque e a formação, as pessoas já não estariam tão conscientes do comportamento de risco que tiveram. Ainda, a formação foi marcada para um dia de semana durante o horário laboral, de acordo com a disponibilidade do formador, previsto ser um ponto positivo para que as pessoas viessem assistir, por outro lado interromper a funções do trabalho pode ter dissuadido de participar.

4.4 Segundo Ataque

O segundo ataque foi realizado em alturas diferentes para os grupos, a campanha dos estudantes decorreu entre 27 de maio e 10 de junho, e a dos funcionários e docentes/investigadores entre 10 e 24 junho. O *e-mail* enviado aos estudantes foi diferente do enviado aos funcionários e docentes/investigadores, a mensagem para este ataque foi específica para cada grupo.

Embora tenham sido redirecionados novamente para um *site* diferente do apresentado, a página a que chegavam era informativa (Anexo 5.1 Figura 79) de como evitar ser vítima, de forma a complementar a campanha, não foi recolhido nenhum campo do *site*. Sendo o último ataque deste projeto, para além de avaliar se as pessoas reconheciam um ataque, também servia como uma última chamada de atenção aquelas que fossem vítimas.

Os dados recolhidos foram comparados com os dados do primeiro ataque, com a exceção do passo de submeter credenciais, como mencionado acima, não foi aplicado neste ataque.

4.4.1 Fase de Preparação

Para este segundo ataque, esta fase só inclui a definição do tipo de *e-mail* a mandar, sendo que a utilização da plataforma Gophish manteve-se, garantindo que ambos os ataques fossem uniformes entre as duas campanhas, e que os dados fossem comparáveis. E as datas embora fossem alteradas foram redefinidas noutras fases do projeto.

Quanto ao *e-mail* elaborado foi específico a cada grupo, usando circunstâncias específicas aos estudantes, e específicas aos funcionários e docentes/investigadores, pode ser considerado um ataque de *spear phishing* (2.1).

4.4.2 Implementação

A implementação deste segundo ataque funcionou de forma semelhante ao primeiro, em que a diferença está na mensagem enviada aos grupos e na página ao qual foram redirecionados, e não nos passos da sua execução.

Execução da Campanha de Phishing

A abordagem para as mensagens foi semelhante ao primeiro ataque, causar sentido de urgência, no entanto o conteúdo não foi tão generalizado. Para os grupos de funcionários e docentes/investigadores a mensagem advertia para novos critérios de avaliação, que teriam sido decididos recentemente e deveriam ser consultados o quanto antes. Nesta mensagem foram feitos alguns erros ortográficos (Figura 16, linha 2), que numa mensagem legítima não deveriam existir. A ligação apresentada era uma variação do *URL* do *site* da universidade que não existe (Figura 16, linha 3), devendo de ser identificado como falso. E ainda como nos outros *e-mails*, o endereço (Figura 16, linha 5) e o serviço falso (Figura 16, linha 7) também serviam como indicadores.

1 Caro(a) Professor(a),

2 Os novos regulamentos foram aprovados no ultimo Concelho e estão em vigor desde
3 o inicio do mês. Deve consultar os novos regulamentos para a avaliação no seguinte
4 endereço:

5 http://www.u.ma.pt/regulamentosavalicao.pdf

6 Atentamente,

7 Direção da Universidade

Figura 16: Modelo de *e-mail* enviado aos funcionários e docentes/investigadores na segunda campanha.

Para os estudantes foi alertado que um processo novo tinha sido começado (Figura 17, linha 2), este processo seria de cancelamento de créditos, seguido do pedido para aceder ao processo (Figura 17, linha 3 e 4). À semelhança do primeiro ataque, o endereço de *e-mail* e o serviço não existente (Figura 17, linha 5) poderiam ser usados como indicadores de que este *e-mail* não era legitímo.

1 Caro(a) Estudante,

2 Deu início ao processo 6351, para cancelamento de créditos.

3 Pode confirmar as informações e seguir o processo através do InfoAlunos acedendo
4 a sua conta: infoalunos.uma.pt

5 Cumprimentos,

6 Apoio Universidade da Madeira

Figura 17: Modelo de *e-mail* enviado aos estudantes na segunda campanha.

Ao criar ambas as mensagens foi tido em conta as indicações enviadas durante a campanha de consciencialização, todos os sinais que eram possíveis identificar no *e-mail* falso da segunda campanha foram baseados nas indicações da apresentação *powerpoint* fornecida.

A página à qual os membros da universidade foram redirecionados foi igual para todos os grupos, foi uma página informativa (Anexo 5.1 Figura 79), começando por explicar que era uma página inofensiva que fazia parte de uma campanha de consciencialização por parte da universidade, seguido de alguns exemplos de indicadores a ter em atenção quando recebem um *e-mail*.

O endereço (<serv.de.apoio@gmail.com>) manteve-se o mesmo, mas o nome da conta passou para Serviços Académicos para a campanha dos alunos, e Direção da Universidade para as campanhas dos funcionários e docentes/investigadores. Esta diferença deve-se ao facto de que os *e-mails* enviados tinham assuntos diferentes, mais específicos a cada grupo.

Neste segundo ataque as campanhas tiveram, à semelhança da primeira campanha, uma duração de quinze dias. Na Figura 18 podemos observar o número de pessoas que abriram o *e-mail* (tenham ou não feito os passos seguintes) em cada dia da duração das campanhas.

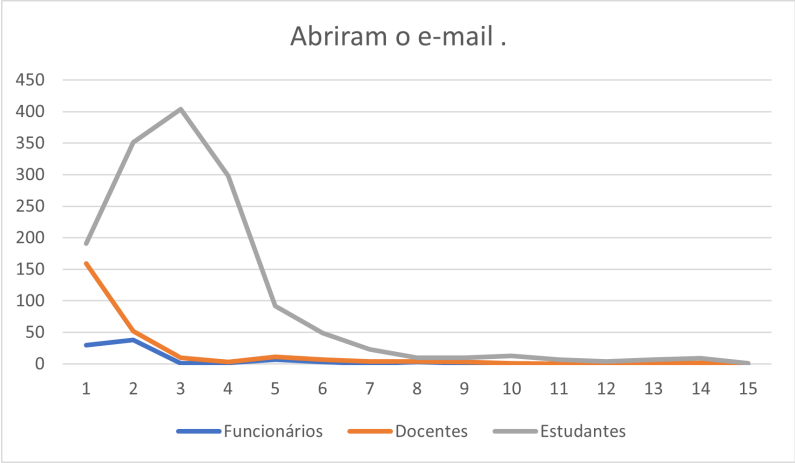

Figura 18: Número por dia de quem abriu o *e-mail* na segunda campanha.

Mais uma vez observamos (Figura 18) que a maior parte dos utilizadores interage com o *e-mail* no dia em que foi enviado. A segunda campanha de cada grupo teve a mesma duração no envio de *e-mails* que a primeira, em que para os funcionários e docentes/investigadores foram enviados em algumas horas num só dia. Podemos observar que os funcionários abriram o *e-mail* em maior quantidade durante os dois primeiros dias, sendo que no segundo o valor foi ligeiramente maior. Os docentes abriram o *e-mail* em maior quantidade durante o primeiro dia. Os *e-mails* dos estudantes foram enviados, mais uma vez, ao longo de quatro dias, e houve maior adesão à abertura do *e-mail* durante os dias dois, três e quatro da campanha.

4.4.3 Resultados

Como referido na secção de resultados da primeira campanha (4.2.3), o Gophish apresenta os dados em três passos (submeter credenciais não é contado neste ataque) pela seguinte ordem:

1. envio do *e-mail* pelo SMTP do Gmail:
2. abertura do *e-mail* (notificação ao Gophish);
3. carregar na ligação no *e-mail* (encaminhamento para a página de alerta).

Os resultados são apresentados no mesmo formato que a primeira campanha:

– frequência absoluta, ou seja, dados absolutos;

– frequência relativa (%), ou seja a percentagem sobre a frequência absoluta;

– frequência relativa (%) em relação ao passo anterior;

Também são apresentados os resultados das pessoas que abriram o *e-mail* informativo, pelo mesmo formato. São apenas contadas as pessoas que abriram o *e-mail*, as que receberam e não abriram não são contabilizadas, pois não demonstram o impacto da informação disponibilizada no *e-mail*.

Resultados globais

Para o segundo ataque, as três campanhas obtiveram os seguintes resultados (Tabela 11): *e-mails* enviados 4431, *e-mails* abertos 1876 (42,08%) e carregaram na ligação 934 (20,95%). A última linha da Tabela 11 frequência em relação ao passo anterior, carregaram na ligação 49,79%.

Tabela 11: Resultados globais da segunda campanha.

E-mails enviados	E-mails Abertos	Carregaram na Ligação
4458	1876	934
-	42,08%	20,95%
-	-	49,79%

Em relação aos resultados globais das pessoas que abriram o *e-mail* informativo (Tabela 12): 540 *e-mails* enviados, 444 (82,22%) *e-mails* abertos, e carregaram na ligação 251 (39,81%), que equivale a 48,42% em relação aos *e-mails* abertos.

Tabela 12: Resultados globais da segunda campanha de quem abriu o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
540	444	215
-	82,22%	39,81%
-	-	48,42%

Resultados de Funcionários

Separando os resultados pelos três grupos obtém-se o seguinte, para os funcionários (Tabela 13): *e-mails* enviados 215, *e-mails* abertos 91 (42,33%), e carregaram na ligação 72 (33,49%). A última linha da Tabela 13 frequência em relação ao passo anterior, carregaram na ligação 79,12%.

Tabela 13: Resultados dos funcionários da segunda campanha.

E-mails enviados	E-mails Abertos	Carregaram na Ligação
215	91	72
-	42,33%	33,49%
-	-	79,12%

Para os funcionários que abriram o *e-mail* informativo (Tabela 14): 15 *e-mails* enviados, 14 (93,33%) *e-mails* abertos, e 13 (86,64%) carregaram na ligação, que equivale a 92,86% em relação aos *e-mails* abertos.

Tabela 14: Resultados dos funcionários da segunda campanha que abriram o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
15	14	13
-	93,33%	86,64%
-	-	92,86%

Resultados de Docentes/Investigadores

Quanto aos docentes e investigadores os resultados foram (Tabela 15): *e-mails* enviados 594, *e-mails* abertos 261 (43,94%) e carregaram na ligação 152 (25,59%). A última linha da Tabela 15 frequência em relação ao passo anterior, carregaram na ligação 58,24%.

Tabela 15: Resultados dos docentes/investigadores da segunda campanha

E-mails enviados	E-mails Abertos	Carregaram na Ligação
594	261	152
-	43,94%	25,59%
-	-	58,24%

Os docentes/investigadores que abriram o *e-mail* informativo (Tabela 16) obtiveram os seguintes resultados: 64 *e-mails* enviados, 47 (73,44%) *e-mails* abertos, e carregaram na ligação 34 (53,13%), que equivale a 72,34% em relação aos *e-mails* abertos.

Tabela 16: Resultados dos docentes/investigadores da segunda campanha que abriram o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
64	47	34
-	73,44%	53,13%
-	-	72,34%

Resultados de Estudantes

Para esta segunda campanha de estudantes não houve problemas com os envios de *e-mails*, embora haja uma diferença de valores, é um valor pequeno (27) em comparação ao total de envios. Como tal as duas campanhas vão ser comparadas sem dar importância a esta diferença.

Portanto os resultados obtidos para os estudantes (Tabela 17) foram: *e-mails* enviados 3649, *e-mails* abertos 1524 (41,76%) e carregaram na ligação 710 (19,46%). A última linha da Tabela 17 frequência em relação ao passo anterior, carregaram na ligação 46,59%.

Tabela 17: Resultados dos estudantes da segunda campanha

E-mails enviados	E-mails Abertos	Carregaram na Ligação
3649	1524	710
-	41,76%	19,46%
-	-	46,59%

Os resultados para os estudantes que abriram o *e-mail* informativo foram os seguintes (Tabela 18): 461 *e-mails* enviados, 383 (83,08%) *e-mails* abertos , e 159 (34,49%) carregaram na ligação, isto equivale a 48,42% em relação aos *e-mails* abertos.

Tabela 18: Resultados dos estudantes da segunda campanha que abriram o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
461	383	159
-	83,08%	34,49%
-	-	41,51%

Outros Resultados

Em relação aos dados pedidos à UCI sobre pedidos de ajuda/esclarecimento nesta campanha só houve dados em relação aos estudantes. Os pedidos de ajuda/esclarecimento feitos foram os seguintes: 4 aperceberam-se e alertaram ao UCI que era *phishing*, 3 solicitaram ajuda/esclarecimento através do *webmaster* e 10 reencaminharam a mensagem ao serviço de apoio ao estudante da universidade pedindo ajuda/esclarecimento. Houve ainda outros serviços da universidade a receber pedidos por *e-mail* e chamadas, mas não foi possível contabilizar quantos estudantes o fizeram.

Durante o segundo ataque houveram 57 respostas diretas ao *e-mail* falso, 1 de um funcionário que se apercebeu do ataque, 1 de um docente/investigador que também se apercebeu do ataque, e as restantes 55 de estudantes. Destas respostas 48 foram a pedir esclarecimento sobre a situação, 1 desconfiou ser um *e-mail* de *phishing* e 6 perceberam que era um ataque.

Foi outra vez visto os acessos à caixa de correio, e os reencaminhamentos das mensagens para outros *e-mails*. Entre os funcionários 26 não acederam à caixa durante a campanha e 4 reencaminham as mensagens. Quanto aos docentes/investigadores 172 não acederam durante a campanha e 44 reencaminham. Para os estudantes 861 não acederam à caixa e 132 reencaminham o *e-mail*.

4.4.4 Análise

A análise dos resultados para o segundo ataque seguirá os mesmos parâmetros que o primeiro, desde o tipo de valores, até a comparação entre grupos. Não é analisado nem comparado o passo credenciais enviadas, pois neste segundo ataque não foi implementado. Será também feita a análise aos resultados das pessoas que receberam e abriram o *e-mail* informativo, é feita a análise global e por grupos. A análise é feita com as pessoas que o abriram e não a todas a quem foi enviado para poder ser avaliado a eficácia deste tipo de método de consciencialização.

Os valores para o número de elementos mantém-se o mesmo para os serviços (Tabela 5) e faculdades e laboratórios (Tabela 6). Para os estudantes apesar da falha previamente referida, diferença de *e-mails* enviados não é significativa, as Tabelas 7, 8 e 9 podem ser usadas como referencia para valores absolutos.

Também é feita a comparação entre os resultados globais e específicos de cada grupo, entre as duas campanhas. É com esta comparação que vai ser avaliado se a campanha teve algum efeito ou não, e se há necessidade de haver mais campanhas no futuro.

Análise Global

A primeira comparação é usando a frequência relativa (%) dos grupos e do resultado global, que pode ser observada na Figura 19. Em todos os grupos a frequência de *e-mails* abertos aumentou em relação ao primeiro ataque (Figura 9). Este aumento significa que o assunto do *e-mail* gerou mais curiosidade em ver o seu conteúdo, visto ser o primeiro elemento que o destinatário lê, o que demonstra que um *e-mail* direcionado é mais efetivo a chamar a atenção das pessoas.

Entre os grupos em si, nenhum grupo se destaca neste passo.

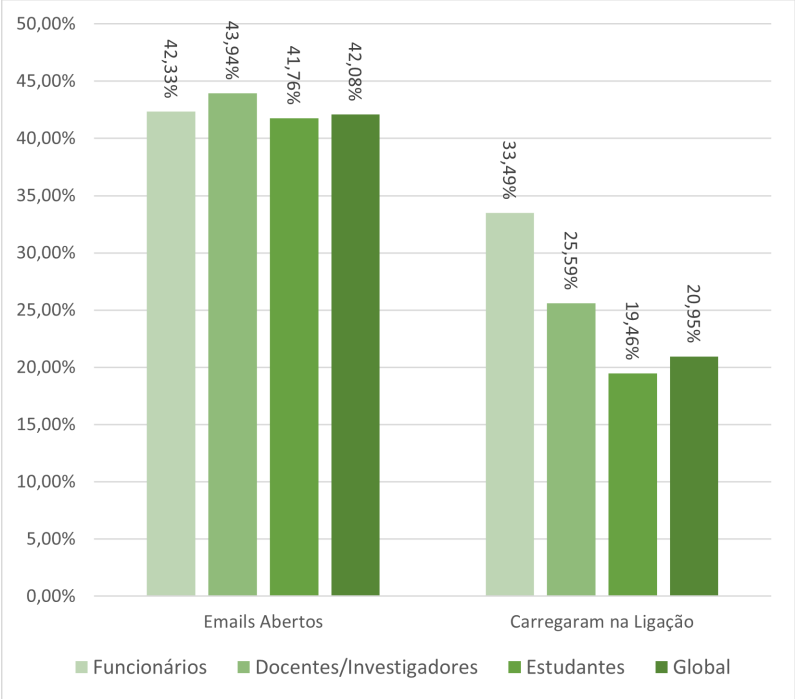

Figura 19: Comparação da frequência relativa (%) dos grupos e do global da segunda campanha.

Para o segundo e último passo, enquanto na primeira campanha (Tabela 9) os funcionários foram os que menos carregaram na ligação e os estudantes os que mais carregaram, na segunda aconteceu o oposto. Os estudantes foram os que menos carregaram com 19,45% (710 estudantes), e os funcionários os que mais carregaram com 33,49% (72 funcionários). Os docentes/investigadores mantiveram-se na mesma posição, mas o valor de pessoas a carregar na ligação aumentou para 25,59% (152 docentes/investigadores).

O resultado dos funcionários e docentes vem salientar a falta de adesão à campanha de consciencialização, principalmente à sessão presencial, onde só estiveram presentes duas pessoas das oitenta e oito convidadas, onde todos os indicadores de um *e-mail* fraudulento integrados neste segundo ataque foram mencionados e exemplificados.

O gráfico da Figura 20 sobre a frequência relativa (%) em relação ao passo anterior, confirma os pontos referidos acima, e também é comparado à primeira campanha (Figura 10). Os funcionários voltaram a ser os que mais carregaram na ligação em relação a quantos abriram o *e-mail*, com 79,12%. Os funcionários, que na primeira campanha tinham sido o grupo que menos carregou na

ligação, passaram a segundo com 58,24%, e os estudantes passaram a ter o valor mais baixo, com 46,59%.

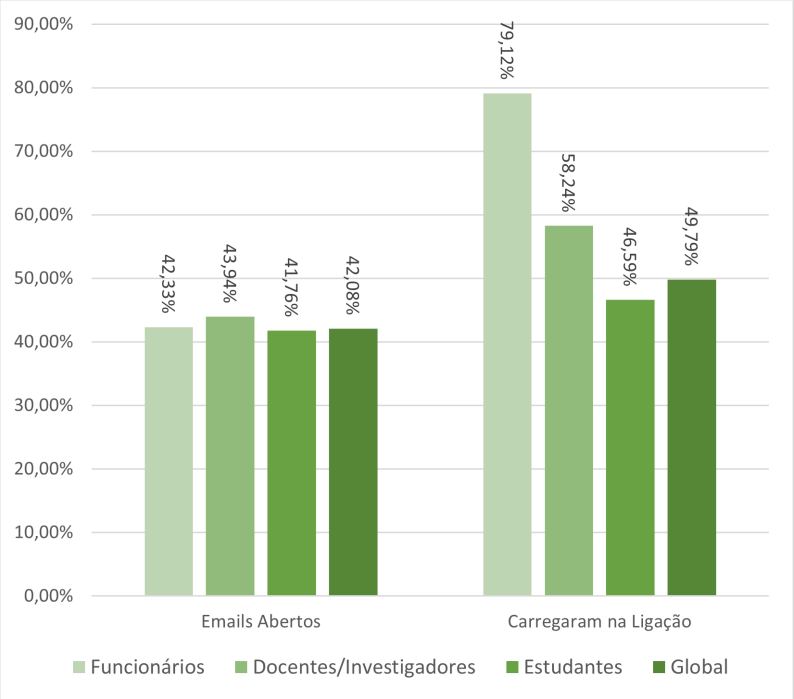

Figura 20: Comparação da frequência relativa (%) em relação ao passo anterior dos grupos e do global da segunda campanha.

Nesta segunda campanha o envio de um *e-mail* direcionado mostrou-se mais eficaz aos funcionários e docentes, visto a que situação escolhida não era do seu controlo, isto é, a mudança dos termos de avaliação realizada pela Direção da Universidade. Enquanto que a situação para os estudantes dependia de ações prévias dos próprios, isto é, iniciar um processo no Infoalunos, o que pode ter ajudado na perceção de o *e-mail* ser fraudulento.

Em relação aos resultados globais (Figura 21) não houve muita diferença entre a frequência de pessoas que carregaram na ligação, com 48,42% nas pessoas que abriram o *e-mail* informativo e 50,21% nas pessoas sem *e-mail* . Apesar de que as pessoas com *e-mail* terem uma percentagem menor a diferença não é significativa, isto demonstra que de forma global o *e-mail* informativo não teve impacto na perceção dos membros da universidade sobre o que é um *e-mail* de *phishing*.

A comparação dos resultados dos grupos mostra que apenas um grupo melhorou, mas sendo este o grupo maior houve uma melhoria no resultado global quanto à primeira campanha, onde 1031 carregaram na ligação (Tabela 1), contra 934 (Tabela 11) na segunda campanha.

Segue-se a análise dos resultados de cada grupo e dos seus parâmetros. Tal como na primeira análise (4.2.4), deste ponto até o fim da análise só é mostrado a frequência relativa (%) em relação ao passo anterior, também será feita a análise de cada grupo em relação às pessoas que receberam e abriram o *e-mail* informativo.

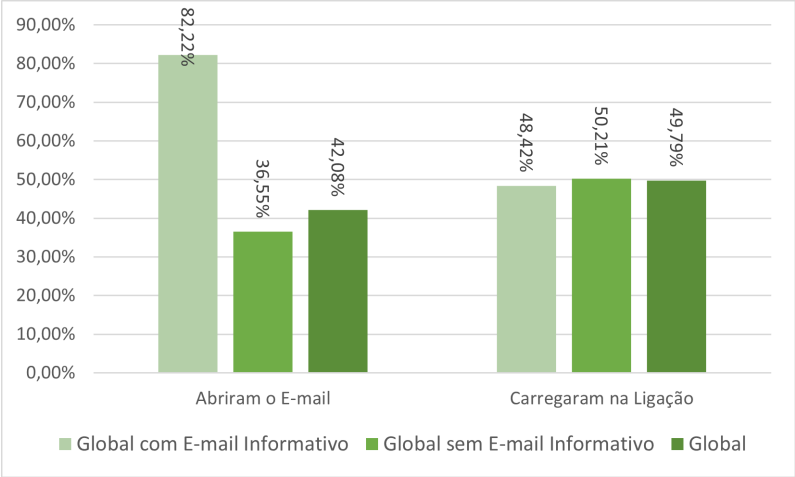

Figura 21: Comparação do global com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

Análise de Funcionários

Começando por analisar os serviços (Tabela 5) aos quais os funcionários pertencem, como esperado pelos resultados da primeira campanha (Figura 11) e comparando com a mesma, todos os serviços tiveram pior desempenho a identificar os sinais de que o *e-mail* era fraudulento (Figura 22). O serviço B e C atingiram os 100% de pessoas que abriram o *e-mail* e também carregaram na ligação, 7 e 4 funcionários, respetivamente. Todos os outros serviços atingiram valores acima dos 70,00%.

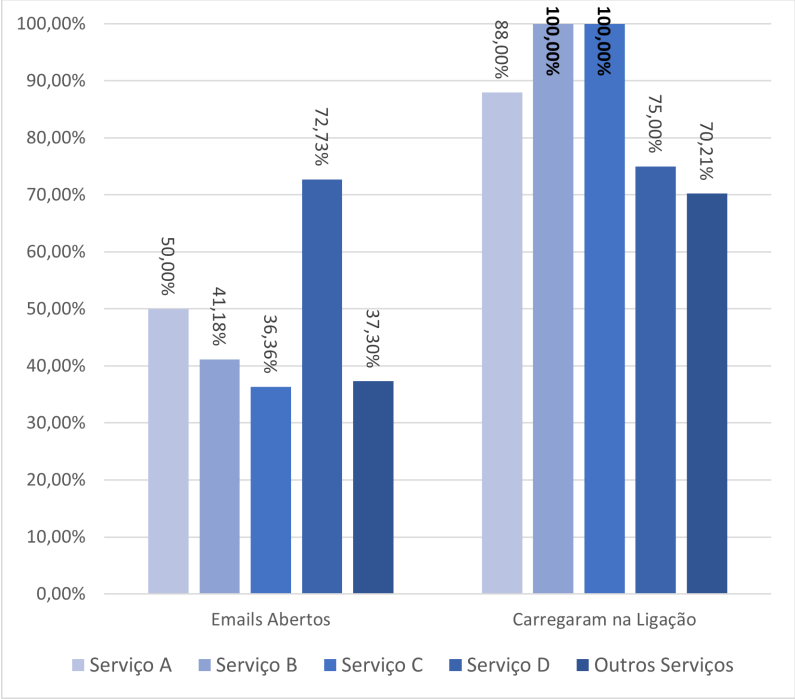

Figura 22: Comparação da frequência relativa (%) em relação ao passo anterior dos funcionários da segunda campanha.

Também referido na primeira análise (4.2.4), a dimensão de alguns dos serviços pode fazer com que estes valores não sejam adequados a analisar, no entanto é de salientar, novamente, que no geral os resultados dos funcionários pioraram, na primeira campanha 32 carregaram na ligação (Tabela 2), na segunda passou a 72 (Tabela 13).

Em relação aos *e-mail* informativo, ao comparar os resultados dos funcionários que o abriram com os resultados dos funcionários sem *e-mail* (Figura 23), os funcionários do *e-mail* informativo mostram pior resultado com 86,67% a carregar na ligação, contra 76,62% em relação aos que não viram. Esta diferença de 10% demonstra que o *e-mail* informativo não teve o impacto desejado.

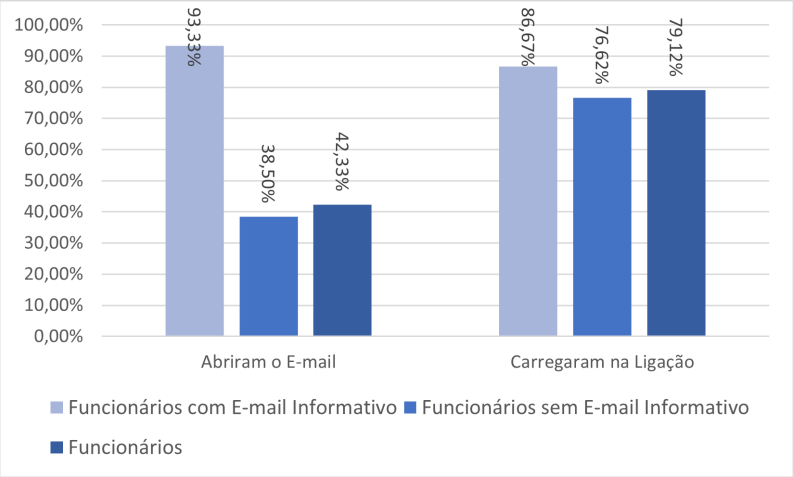

Figura 23: Comparação de funcionários com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

Os resultados dos funcionários demonstram que o *e-mail* não é uma forma efetiva de os educar para reconhecer ataques de *phishing*, mesmo que a pessoa veja a mensagem, há a possibilidade de não aceder aos recursos que continham informação. Estes resultados também refletem a falta de adesão à sessão presencial, que ao contrario do *e-mail* garante que a pessoa vai ser informada sobre os vários indicadores de que uma mensagem é fraudulenta.

Análise de Docentes/Investigadores

A análise das faculdades e laboratórios (Figura 24) do grupo dos docentes/investigadores, quando comparada com a primeira campanha (Figura 12), mostra que enquanto algumas faculdades e laboratórios melhoraram, outros atingiram valores mais altos. Apenas a Faculdade B e o Laboratório A destacam-se pelo valor de frequência baixo, com 43,64 % (24) e 25,00% (4).

As restantes faculdades e laboratórios, apesar de algumas melhorias, tal como os funcionários, continuam a demonstrar dificuldades em identificar os sinais indicadores de um *e-mail* falso, sendo que no geral o grupo passou de 114 (Tabela 3) a carregar na ligação na primeira campanha, a 152 (Tabela 15) na segunda.

Após a análise dos resultados de ambos os ataques, no grupo dos docentes/investigadores, não há uma resposta definitiva se há pessoas de uma área profissional que são mais vulneráveis aos

ataques. Em ambos os ataques as várias faculdades e laboratórios demonstraram que contam com pessoas com tendências a comportamentos de risco.

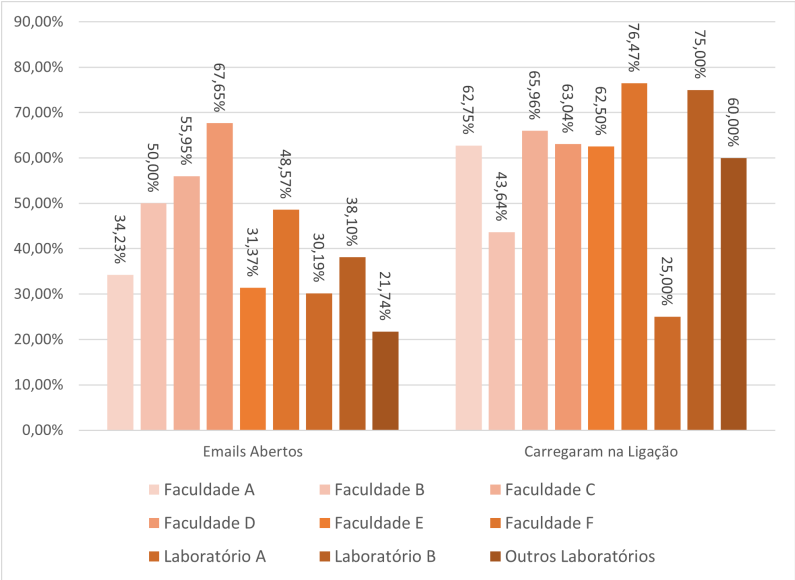

Figura 24: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e laboratórios dos docentes/investigadores da segunda campanha.

Entre os docentes/investigadores que viram o *e-mail* informativo e os sem *e-mail* informativo (Figura 25), observa-se o mesmo que aconteceu com o grupo funcionários, em que carregaram na ligação com *e-mail* 72,34%, um valor mais elevado que os 55,14% sem *e-mail*. Mais uma vez quem teve acesso ao *e-mail* teve pior resultado, sendo que o grupo docentes/investigadores teve uma diferença mais significativa entre as duas amostras com 17%.

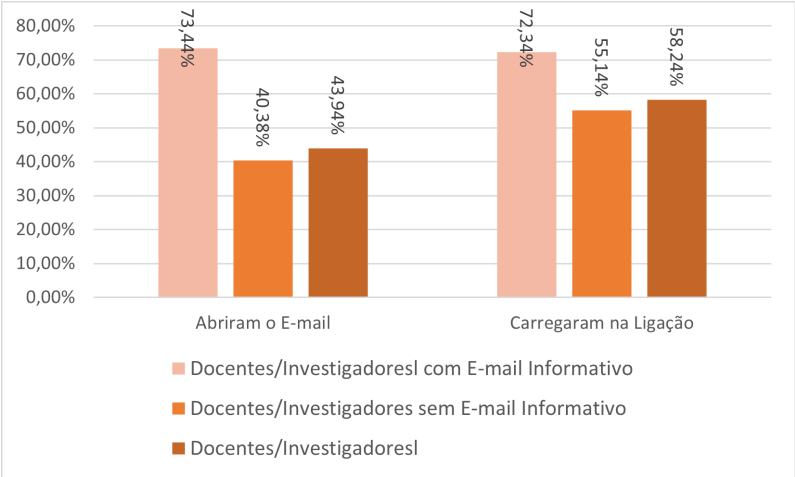

Figura 25: Comparação global com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

Podem ser tiradas as mesmas conclusões entre os funcionários e os docentes/investigadores, ambos obtiveram piores resultados na segunda campanha, também não houve adesão por parte

dos docentes/investigadores à sessão presencial, e mesmo que abram o *e-mail* informativo não garante que leiam os recursos, o que significa que o *e-mail* não é um método de consciencialização efetivo.

Análise de Estudantes

Por último, segue-se a análise dos resultados das faculdades e escolas (Tabela 7), dos ciclos (Tabela 8) e dos anos (Tabela 9) para o grupo dos estudantes.

Em ambos os casos na análise de faculdades (Figura 26) e de ciclos (Figura 27), mesmo com o aumento de estudantes a abrir o *e-mail*, houveram menos estudantes a carregar na ligação, em comparação com o primeiro ataque (Figuras 13 e 14). Esta melhoria indica que os estudantes no geral tiveram mais facilidade em identificar que o *e-mail* era falso, através dos vários indicadores. O número de estudantes a carregar na ligação passou de 885 na primeira campanha (Tabela 4) a 710 na segunda (Tabela 17).

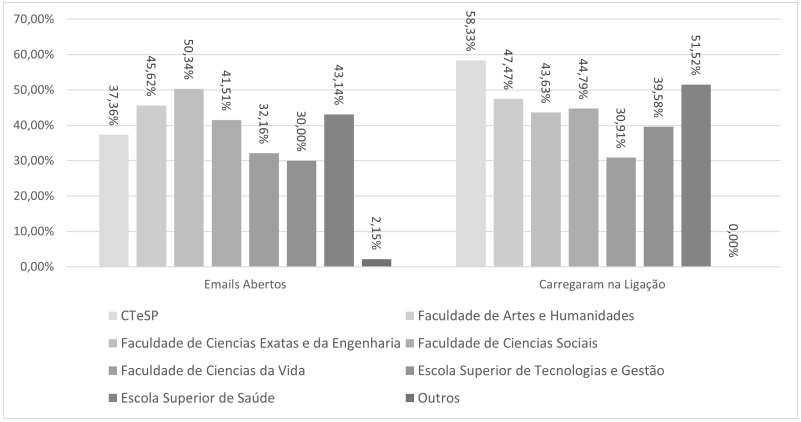

Figura 26: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e escolas dos estudantes da segunda campanha.

Neste segundo ataque mais uma vez não se distingue-se nenhuma faculdade ou escola em relação a comportamentos de risco, sendo que a ESTG teve o valor mais baixo, com 30,91%, que equivale a 15 pessoas, enquanto que as restantes faculdades e escolas têm valores próximos. Tendo em conta os resultados de ambos os ataques (Figura 13 e Figura 26) podemos concluir que a área de estudo não influência aquando da prevenção de ataques.

Na primeira análise em relação ao ciclo (Figura 14) tinha sido observado que os estudantes mais novos, tinham mais tendência a comportamentos de risco em comparação aos estudantes mais antigos. Neste ataque em relação aos ciclos, os CTeSP é o ciclo com maior frequência no passo de carregar na ligação (Figura 27). Já a diferença entre o 1º, 2º e 3º ciclos é mínima, sendo necessário relembrar que para o 3º os 42,86% equivalem apenas a 12 pessoas, quando comparado aos 44,99% do 1ºciclo e 44,47% do 2º ciclo, que equivalem a 493 e 78 pessoas, respetivamente.

Por fim, o último parâmetro a analisar são os anos por ciclo (Figura 28), embora no geral os resultados melhoraram, havendo menos pessoas a carregar na ligação, ao contrario da primeira análise (Figura 15) os últimos anos de cada ciclo tiveram os piores resultados.

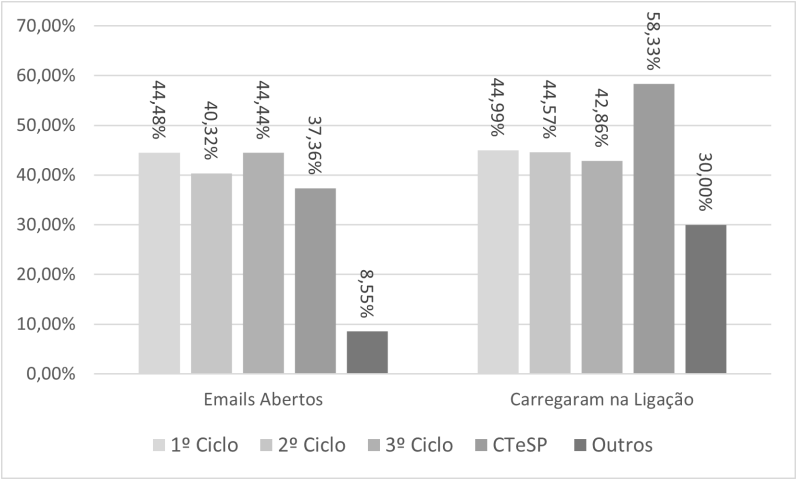

Figura 27: Comparação da frequência relativa (%) em relação ao passo anterior dos ciclos dos estudantes da segunda campanha.

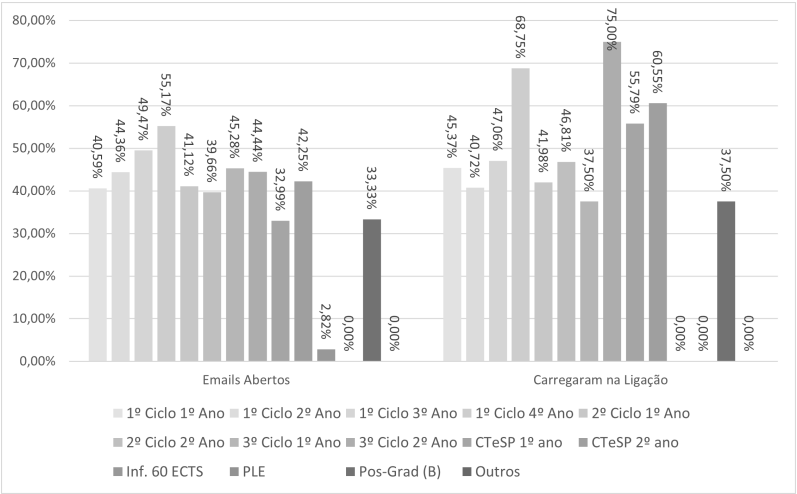

Figura 28: Comparação da frequência relativa (%) em relação ao passo anterior dos anos dos estudantes da segunda campanha.

A comparação entre os estudantes com *e-mail* informativo e estudantes sem o *e-mail* (Figura 29), demonstra que estudantes com *e-mail* obtiveram melhores resultados com 43,11% contra 48,69%, no entanto é uma diferença de apenas 5%, não sendo o suficiente para atribuir esse resultado ao impacto do *e-mail*.

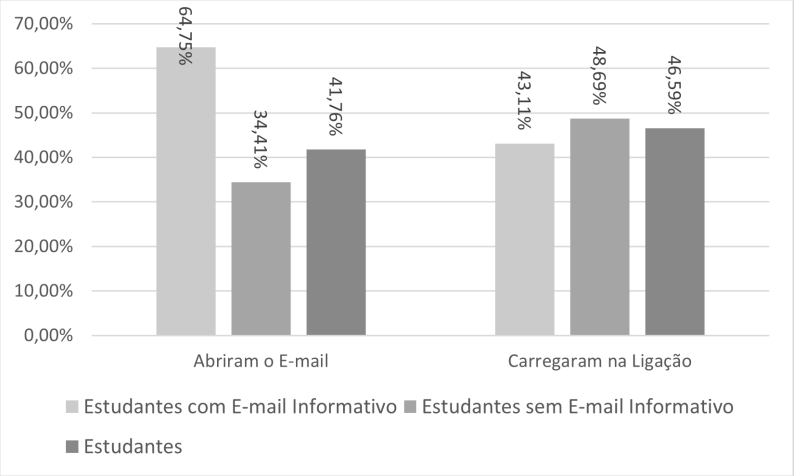

Figura 29: Comparação da frequência relativa (%) em relação ao passo anterior dos grupos e do global da segunda campanha.

Para os estudantes podemos concluir que a área de estudo não afeta os resultados em nenhuma campanha, os ciclos para esta segunda campanha não mostraram grandes diferenças entre si ao contrario da primeira campanha, com a exceção dos CTeSP que apresentaram o valor mais alto, sendo que representam uma parte da faixa de alunos mais novos. Em relação aos resultados dos estudantes com *e-mail* informativo e sem *e-mail*, a diferença é pequena, não garantido que os resultados sejam influenciados pela receção do *e-mail*.

Conclusões da Análise

Tanto para os funcionários como para os docente/investigadores, após a comparação de ambas as campanhas, não há indícios de que a área de serviço influencie a perceção do que é um *e-mail* fraudulento. Já para os estudantes, na comparação de ambas as campanhas não há diferenças significativas entre as faculdades e escolas, ou seja a área de estudo não afeta. No entanto existe diferenças em relação ao ciclo, sendo que os ciclos mais baixos (1ºciclo e CTeSP) tiveram piores resultados.

Houve dificuldades na análise de alguns serviços em relação aos funcionários, e de faculdades e laboratórios para os docentes/investigadores, onde a amostra para envio de *e-mails* era mais pequena, e não havendo adesão aquando de abrir os *e-mails* durante os ataques, a amostra final para a análise dos resultados não era suficiente para tirar conclusões.

É difícil avaliar o impacto do *e-mail* informativo na segunda campanha, pois não há informações se as pessoas acederam aos recursos disponibilizados. Apesar da comparação entre utilizadores com acesso ao *e-mail* e sem acesso, outros fatores podem ter mais influência nos resultados.

De modo geral, apesar de haver melhorias no grupo dos estudantes e de a página à qual os grupos foram redirecionados ser informativa, é importante continuar a realçar a importância de

informar-se sobre Cibersegurança, Engenharia Social e os seus ataques. O facto de que um número elevado de estudantes (710) ainda carregou na ligação e de que os resultados dos restantes grupos pioraram, demonstra a necessidade de mais campanhas de consciencialização.

4.5 Outras Considerações

São aqui apresentadas algumas situações que ou não foram consideradas no planeamento, que foram consideradas mas não podiam ser controladas, ou que só foram notadas após o ataque.

Durante os testes foi notado que os *e-mails* enviados pelo Gophish, quando é selecionado para serem enviados ao longo de um período de tempo (foi feito para as 6 campanhas ao longo dos 2 ataques), são enviados de forma uniforme ao longo do período definido, não podendo decidir as horas específicas em que sejam enviados. Isto significa que para os estudantes, que são o grupo de maior dimensão, os *e-mails* foram enviados ao longo de três dias, alguns deles foram enviados em horário pós-laboral, podendo ser um indicador que estes não eram legítimos, no entanto foi mantido o envio desta forma para não sobrecarregar o servidor de *SMTP*.

Para além do horário de envio, o dia poderia ser um indicador, visto que alguns dos dias em que decorreram os ataques os serviços da universidade não estavam disponíveis. Para os funcionários e docentes/investigadores o segundo ataque foi feito num feriado, facto que só foi notado após o início de cada campanha, não podendo ser alterado, já para os estudantes em ambas campanhas houveram *e-mails* a ser enviados durante o fim-de-semana.

Algo que não podia ser controlado eram os filtros de *e-mails* que não pertenciam ao domínio da universidade, para aqueles membros que reencaminham os seus *e-mails*, não é garantido que não tivesse ido para a pasta de *spam* ou lixo, visto tal ter acontecido em alguns dos testes realizados anteriormente.

Na primeira campanha, apesar de todas as credenciais enviadas terem sido contadas para o resultado final, existe a possibilidade de haver credenciais falsas, de pessoas que reconheceram que a página era falsa (ou até mesmo o *e-mail*). Como a palavra passe não foi recolhida, e como a única maneira de verificar cada utilizador era manualmente, havendo um número grande de submissões (total da primeira campanha 697), foi decidido não avaliar este facto.

Em ambas as campanhas alguns existem fatores que não podem ser controlados nem contabilizados para os resultados. Um fator é difusão de informação sobre os *e-mails*, isto é, no caso das pessoas que aperceberam-se que o *e-mail* era de *phishing*, podem ter avisado aos seus colegas, estes colegas em principio já não iriam carregar na ligação. Outro fator é a informação externa à campanha da universidade, isto é, conhecimentos ganhos através de outras campanhas ou de alertas para ter atenção ao *phishing*, dados por terceiros, por exemplo: serviços, instituições, bancos a alertar que estão a ser enviados *e-mails* fraudulentos em seu nome.

A última situação a não ser considerada durante o planeamento foram as respostas ao *e-mail*, que já foram apresentados os valores no secção de resultados em ambos os ataques (4.2.3, 4.4.3). Acabou sendo uma situação interessante, devido ao conteúdo de alguns *e-mails*, desde pessoas a revelar alguns dados e informações pessoais, à confirmação de que algumas pessoas aperceberam-se que era um ataque.

4.6 Conclusões

Após a análise da segunda campanha e tendo em conta a os resultados da primeira, pode ser concluído que para os funcionários e docentes/investigadores não há um serviço ou área que influencie os resultados. Em ambas as campanhas, apesar de alguns serviços, faculdades e laboratórios terem melhores resultados que outros, a diferença não foi significativa, considerando também que em alguns casos o tamanho da amostra acabou por não ser grande o suficiente para ter um análise rigorosa.

Já os estudantes em ambas as campanhas tiveram piores resultados em ciclos mais baixos, mostrando que a idade ou a experiência dentro de uma instituição pode afetar a perceção de um *e-mail* fraudulento.

Quanto às diferenças de resultados entre ambos os ataques, no segundo ataque os funcionários e docentes/investigadores obtiveram piores resultados, e os estudantes obtiveram resultados melhores. A segunda mensagem enviada era mais específica para cada grupo do que a primeira, o que pode ter influenciado os resultados.

Quanto à campanha de consciencialização, a adesão tanto ao *e-mail* informativo quanto à sessão de formação não foi a esperada, talvez devido ao tempo que passou entre o primeiro ataque e a campanha, ou mesmo pela falta de interesse dos membros da comunidade académica no tema de Engenharia Social.

No geral é necessário continuar a educar os membros da universidade através dos vários métodos usados na campanha de consciencialização. Usando os ataques para demonstrar o quão vulneráveis os membros da universidade são e quais são os seus comportamentos de risco, esperando desta forma incentiva-los a aderir e a participar nos métodos de consciencialização.

5 Conclusão

O estudo dos casos de ataques de *phishing* e via *pens USB* na Universidade da Madeira mostrou que ainda existe uma grande falta de conhecimento sobre a Engenharia Social, e que os membros da comunidade académica estão vulneráveis a este tipo de ataques. Nos três grupos analisados, funcionários, docentes/investigadores e estudantes, foi observado a dificuldade em reconhecer os sinais que indicavam que estavam a ser alvos de um ataque.

O ataque via *pens* não obteve o alcance inicialmente planeado, acabando por ter uma amostra pequena de *pens* espalhadas, e embora tenham sido obtidos alguns resultados, não são suficientes para fazer uma análise mínima sobre a perceção da comunidade académica a estes ataques. Outro problema foi as pessoas que inseriram a *pen* e abriram os ficheiros, não responderam ao questionário disponibilizado. Desta forma não foi possível entender o porquê das pessoas interagirem com as *pens* e o quão vulneráveis estão as estes ataques.

O ataque de *phishing* teve um maior impacto, com os resultados a permitirem analisar os vários parâmetros decididos para cada grupo. Nos funcionários foram analisados variações entre serviços, nos docentes/investigadores foram analisadas diferenças entre as faculdades/escolas e laboratórios, e nos estudantes foram analisadas as diferenças entre faculdades/escolas, ciclos e anos de inscrição. No entanto foi observado que entre os parâmetros, aqueles com menos elementos, ou onde a adesão ao passo de abrir o *e-mail* foi menor, produziram amostras demasiado pequenas para que a análise fosse representativa das pessoas dessas categorias. Muitas vezes os resultados ou eram muito superiores aos restantes, ou muito inferiores. Já as amostras maiores permitem uma melhor perceção da realidade, aquando de comparar as várias categorias, com o objetivo de perceber quais as mais vulneráveis.

A análise dos resultados do grupo dos funcionários foi a que deu mais dificuldades, em que a maior parte dos serviços não continham mais de dez funcionários, acabando por não ter sido viável a comparação entre os serviços, não sendo possível identificar o serviço mais vulnerável. No entanto, tendo em conta os serviços onde foi possível analisar, foi observado que não há relação entre o serviço e ser mais vulnerável a um ataque de *phishing*.

Os resultados do grupo docentes/investigadores não demonstrou que existisse relação entre a área profissional, ou seja, faculdade e laboratório a que pertence, e a tendência em ser vítima de um ataque de *phishing*.

Quanto aos estudantes, com a análise dos resultados foi verificado que o ciclo e o ano afetava os comportamentos de risco, onde os ciclos e anos com estudantes mais novos foram identificados como os mais vulneráveis. Já na comparação entre faculdades e escolas, não foi identificada nenhuma relação entre a área de estudo, e a tendência a comportamentos de risco.

Quanto aos resultados globais, houve uma melhoria entre o primeiro e o segundo ataque, mas deveu-se ao facto de que o grupo com maior amostra (estudantes) tenha melhorado entre os dois ataques. Já os funcionários e docentes/investigadores obtiveram piores resultados.

Durante a campanha de consciencialização os métodos implementados foram cartazes, *e-mail* informativo e sessão de formação. Os cartazes serviram como primeiro alerta para Cibersegurança, nenhuma informação foi proporcionada. O *e-mail* informativos forneciam recursos para aprofundar os conhecimentos de Cibersegurança. E a sessão de formação foi realizada focando-se apenas no *phishing*.

Os *e-mails* informativos, que foram enviados apenas a quem carregou na ligação e enviou credenciais no primeiro ataque, é o método com mais alcance, não havendo limitação na quantidade de pessoas às quais este pode ser dirigido. No entanto não permite avaliar se algum conhecimento realmente é transmitido, não há como garantir que quem o recebe o vai abrir, e mesmo que o abram, visitar e descarregar os recursos fornecidos depende do interesse das pessoas no tema.

A sessão de formação daria a oportunidade de educar as pessoas de forma mais direta, ensinando o conceito de engenharia social e de *phishing*, mostrando os sinais de que um *e-mail* é fraudulento, e o mais importante, a vantagem de uma sessão presencial, partilhar experiências passadas e tirar dúvidas. Porém os funcionários e docentes/investigadores não aderiram à participação na mesma, isto pode dever-se ou à falta de interesse no tema, ou ao facto de que foi feito no horário laboral, que significa que o horário poderia não ser compatível com as suas tarefas ou aulas. Neste último caso é fundamental que a própria universidade incentive e coordene com os funcionários e com os docentes/investigadores, de modo a possibilitar a participação nas sessões.

A maior dificuldade na prevenção da Engenharia Social é dar a entender às pessoas a importância de se informarem e de se educarem em relação aos ataques. Como observado ao longo deste projeto ainda há falta de disposição (ou tempo) em aprender novos conceitos, mesmo que estes sejam para o benefício da própria pessoa. É preciso dispor de vários métodos de consciencialização para que uma campanha alcance o maior número de pessoas e para assegurar-se de que estas realmente adquiram novos conhecimentos.

5.1 Trabalho Futuro

Futuramente ambos a campanha de consciencialização e os ataques simulados devem ser regulares. A evolução da tecnologia faz com que o aparecimento de novas técnicas de ataque seja cada vez mais frequente, sendo necessário que a educação sobre Cibersegurança, focada na Engenharia Social, torne-se contínua para os membros da universidade mais antigos. Também sendo necessário garantir que os novos membros sejam educados em conjunto com os antigos.

Para que a campanha de consciencialização tenha mais adesão, para além dos meios aplicados neste projeto, poderão se aplicados outros métodos que incentivem as pessoas aprender mais sobre o tema. Outro fator é a realização de mais ataques simulados antes e depois da campanha, de forma a salientar o quão vulneráveis as pessoas estão a ataques reais e avaliar o impacto da campanha.

Também poderão ser elaborados mais formulários para antes e depois da campanha. Desta forma será mais fácil perceber qual é a perceção que os membros da universidade têm sobre Engenharia Social, os tipos de ataques e os seus próprios conhecimentos. Estes dados permitirão realizar uma campanha de consciencialização mais direcionada aos membros da universidade, ao se focar em específico nas suas dificuldades e falta de conhecimentos. O formulário após a campanha de consciencialização permitirá avaliar se os participantes acharam a campanha adequada, se ganharam mais conhecimentos, se estão preparados para evitar os ataques e quais as melhorias a fazer à própria campanha.

No caso do *phishing*, junto aos *e-mails* informativos e à sessão de formação, para que as pessoas possam aplicar as formas de identificação de ataques, poderão ser usados jogos. Estes têm como objetivo confrontar os seus utilizadores com exemplos de *e-mails* que poderão receber no dia-a-dia, e identificar se são válidos ou não. Este método tem-se mostrado eficiente na prevenção de *phishing*, sendo necessário pesquisar os vários jogos pré-existentes para escolher aquele que mais se adequa ao

contexto universitário. No caso de não haver um jogo adequado, há a possibilidade de desenvolver um jogo no contexto de uma universidade ou instituição de ensino.

Ainda para o *phishing*, na realização de novos ataques, deverão ser aplicadas diferentes técnicas como, em vez de criar uma situação em que as pessoas devam carregar numa ligação, podem ser adicionados anexos à mensagem, para fazer a verificação de quantas pessoas descarregam os ficheiros. Também pode ser criada uma mensagem onde é pedido que as pessoas enviem os seus dados diretamente por *e-mail*, sendo que neste caso é necessário fazer *e-mails* direcionados (*spear phishing*), ainda mais específicos para os diferentes cargos na universidade, ou até mesmo, no caso dos estudantes, para os diferentes cursos.

No caso dos ataques via *pens USB* deverá ser dada mais informação sobre como diferentes dispositivos *USB* podem ser usados para realizar ataques e formas de verificar se estes dispositivos foram alterados ou se contêm ficheiros maliciosos.

Para os ataques simulados via *pens USB* a realização de um ataque terá de ser feita com um número maior de *pens*, que possam ser distribuídas pelo edifício da universidade, e talvez distribuí-las pelos restantes pólos da Instituição, como o Colégio dos Jesuítas, onde se encontram vários serviços da universidade, como a reitoria.

Também em vez de as usar com a sua configuração de *pen drives*, estas podem ser alteradas para que sejam identificadas como outro tipo de dispositivo *USB*, de maneira que corram automaticamente quando inseridas num computador. Além disso podem ser utilizados outros dispositivos *USB* para realização dos ataques, desta forma não é preciso que a pessoa abra um ficheiro e pode ser avaliado só a ação de inserir os dispositivos de fontes desconhecidas num computador.

Referências

[1] I. B. Michael Veale, "Cybersecurity," *Internet Policy Review*, vol. 9, no. 4, pp. 1–22, 2020.

[2] J.-M. Chenou, "The contested meanings of cybersecurity: evidence from post-conflict Colombia," *Conflict, Security Development*, vol. 21, no. 1, pp. 1–19, 2021.

[3] D.-T. N. P. R. Craigen, D., "Defining Cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, pp. 13–21, 2014. [Online]. Available: http://timreview.ca/article/835

[4] L. S. Zuoguang Wang, Hongsong Zuoguang, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," *IEEE Access*, vol. 9, pp. 11 895–11 910, 2021.

[5] S. L. Garfinkel, "The cybersecurity risk," *Communications of the ACM*, vol. 55, no. 6, pp. 29–32, 2012.

[6] F. A. R. S. N. Hidayah Zulkiffli, M. N. Ahmad Zawawi, "Passive and Active Reconnaissance: A Social Engineering Case Study," *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, p. 138–143, 2020.

[7] A. J. F. S. N. K. M. R. Arabia-Obedoza, G. Rodriguez, "Social Engineering Attacks A Reconnaissance Synthesis Analysis," *2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, p. 0843–0848, 2020.

[8] L. S. Z. Wang, H. Zhu, "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," *IEEE Access*, vol. 9, p. 85094–85115, 2020.

[9] ——, "Defining Social Engineering in Cybersecurity," *IEEE Access*, vol. 8, p. 11895–11910, 2021.

[10] P. J. S. Nabie Y. Conteh, "Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research*, vol. 6, no. 23, pp. 37–38, 2016.

[11] M. D. R. Dr Nabie Y Conteh, "The Rise in Cybercrime and the Dynamics of Exploiting the Human Vulnerability Factor," *International Journal of Computer Engineering and Applications*, vol. 20, no. 1, p. 12, 2016.

[12] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches," *Future Internet*, vol. 12, no. 10, p. 168, 2020.

[13] C. L. T. Kang Leng Chiew, Kelvin Sheng Chek Yong, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106, pp. 1–20, 2018.

[14] B. B. G. Ankit Kumar Jain, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, pp. 1–39, 2021.

[15] N. Akbar, "Analysing persuasion principles in phishing emails," 2014.

[16] M. N. N. Dorel Paraschiv, Liviu Toader, "Internet Fraud and Phishing Attacks - a European Perspective," *7th BASIQ International Conference on New Trends in Sustainable Business and Consumption*, pp. 394–400, 2021.

[17] APWG, "Phishing activity trends reports," https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf, Acedido a 11 de fevereiro de 2023.

[18] ——, "Phishing activity trends reports," https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf, Acedido a 11 de fevereiro de 2023.

[19] G. P. E. L. Hossein Abroshan, Jan Devos, "COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic," *IEEE Access*, vol. 9, pp. 121 916–121 929, 2021.

[20] E. E. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Science*, vol. 3, no. 1, p. 9, 2014.

[21] A. M. T. C. M. F. C. Giuseppe Desolda, Lauren S. Ferro, "Human Factors in Phishing Attacks: A Systematic Literature Review," *ACM Computing Surveys*, vol. 54, no. 8, pp. 1–35, 2021.

[22] S. M. B. Dr M Nazreen Banu, "A Comprehensive Study of Phishing Attacks," p. 4, 2013.

[23] B. A. Vanessa Gomes, Joaquim Reis, "Social Engineering and the Dangers of Phishing," *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–7, 2020.

[24] S. M. B. Dr M Nazreen Banu, "An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage," *2019 5th International Conference on Information Management (ICIM)*, pp. 82–89, 2019.

[25] M. N. Dung Vu Pham, Ali Syed, "Universal serial bus based software attacks and protection solutions," *Digital Investigation*, vol. 7, no. 3-4, pp. 172–184, 2011.

[26] L. d. N. Tobias Mueller, Ephraim Zimmer, "Using Context and Provenance to defend against USB-borne attacks," *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–9, 2019.

[27] H. S. J. Oliveira, P. Pinto, "Distributed Architecture to Enhance Systems Protection against Unauthorized Activity via USB Devices," *Journal of Sensor and Actuator Networks*, vol. 10, no. 1, p. 19, 2021.

[28] M. P. F. Griscioli, "USBCaptchaIn: Preventing (un)conventional attacks from promiscuously used USB devices in industrial control systems," *Journal of Computer Security*, vol. 29, pp. 51–76, 2021.

[29] P. R. Marie Baezner, "Stuxnet," *CSS Cyberdefense Hotspot Analyses*, vol. 4, p. 16, 2017-10-18.

[30] Y. E. N. Nissim, R. Yahalom, "USB-based attacks," *Computers Security*, vol. 70, pp. 675–688, 2017.

[31] M. T. et al, "Users Really Do Plug in USB Drives They Find," *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 306–319, 2016.

[32] G. S. Hussain Aldawood, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," *Future Internet*, vol. 11, no. 3, p. 73, 2019.

[33] ——, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pp. 62–68, 2018.

[34] W. P. M. J. P. H. H. Jan-Willem H. Bullée, Lorena Montoya, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," *Journal of Experimental Criminology*, vol. 11, no. 1, pp. 97–115, 2015.

[35] D. D. C. A. J. Burns, M. Eric Johnson, "Spear phishing in a barrel: Insights from a targeted phishing campaign," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 1, pp. 24–39, 2019.

[36] W.-S. L. F. A. J. R. M. William Yeoh, He Huang, "Simulated Phishing Attack and Embedded Training Campaign," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 802–821, 2022.

[37] S. V. H. T. V. B. S. L. Gokul CJ, Sankalp Pandit, "PHISHY - A Serious Game to Train Enterprise Users on Phishing Awareness," *CHI PLAY '18: The annual symposium on Computer-Human Interaction in Play*, pp. 169–181, 2018.

[38] A. Darem, "Anti-Phishing Awareness Delivery Methods," *Engineering, Technology Applied Science Research*, vol. 11, no. 6, pp. 7944–7949, 2021.

[39] Y. L. Chengzhi Sun, Jiyu Lu, "Analysis and Prevention of Information Security of USB," *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)*, pp. 25–32, 2021.

[40] H. S. Annette Tetmeyer, "Security Threats and Mitigating Risk for USB Devices," *IEEE Technology and Society Magazine*, vol. 29, no. 4, pp. 44–49, 2010.

[41] S. L. Nalin Asanka Gamagedara Arachchilage, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304–312, 2014.

[42] J. B. Andy Luse, "Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering," p. 13, 2020.

[43] K. N. U. B. D. C. K. E. F. S. A. M. S. Eric B Blancaflor, Adrian B Alfonso, "Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools," p. 10, 2021.

Anexos

Anexos A - Gráficos e Tabelas de Resultados

Este anexo está dividido pelos resultados do primeiro e segundo ataque de *phishing*. Neste capítulo serão apresentados os resultados da campanha, começando com os resultados globais, seguidos dos resultados de cada grupos. A apresentação dos resultados dos grupos será feita pela seguinte ordem: funcionários, docentes/investigadores e, por fim, os estudantes.

Os dados recolhidos pelo Gophish são apresentados em quatro passos, sendo esta a ordem dos acontecimentos:

1. envio do *e-mail* pelo SMTP do Gmail:
2. abertura do *e-mail* (notificação ao Gophish);
3. carregar na ligação no *e-mail* (encaminhamento para a página falsa do Gophish);
4. submeter credenciais (cópia de página de login).

Assim, se alguém submeteu as credenciais, implica ter feitos os outros passos todos e o mesmo aplica-se aos passos restantes. Os resultados de cada passo são apresentados em três linhas:

- frequência absoluta, ou seja, dados absolutos;
- frequência relativa (%), ou seja a percentagem sobre a frequência absoluta;
- frequência relativa (%) em relação ao passo anterior;

Isto é, credenciais enviadas em relação a carregaram na ligação, carregaram na ligação em relação a *e-mails* abertos, e neste caso *e-mails* abertos em relação aos *e-mails* enviados mantém o mesmo valor que da frequência relativa (%).

Também são apresentados gráficos que demonstração, por dia, quantas pessoas realizaram cada passo.

Resultados da Primeira Campanha

Tabela 19: Resultados globais da primeira campanha.

E-mails enviados	**E-mails Abertos**	**Carregaram na Ligação**	**Credenciais Submetidas**
4431	1605	1031	697
-	36,22%	23,27%	15,73%
-	-	64,24%	67,60%

Tabela 20: Resultados dos funcionários da primeira campanha.

E-mails Enviados	E-mails Abertos	Carregaram na Ligação	Credenciais Submetidas
215	60	32	19
-	27,91%	14,88%	8,84%
-	-	53,33%	59,38%

Tabela 21: Resultados dos docentes/investigadores da primeira campanha.

E-mails Enviados	E-mails Abertos	Carregaram na Ligação	Credenciais Submetidas
594	224	114	69
-	37,71%	19,19%	11,62%
-	-	50,89%	60,53%

Tabela 22: Resultados dos estudantes da primeira campanha.

E-mails Enviados	E-mails Abertos	Carregaram na Ligação	Credenciais Submetidas
3622	1321	885	609
-	36,47%	24,43%	16,81%
-	-	66,99%	68,81%

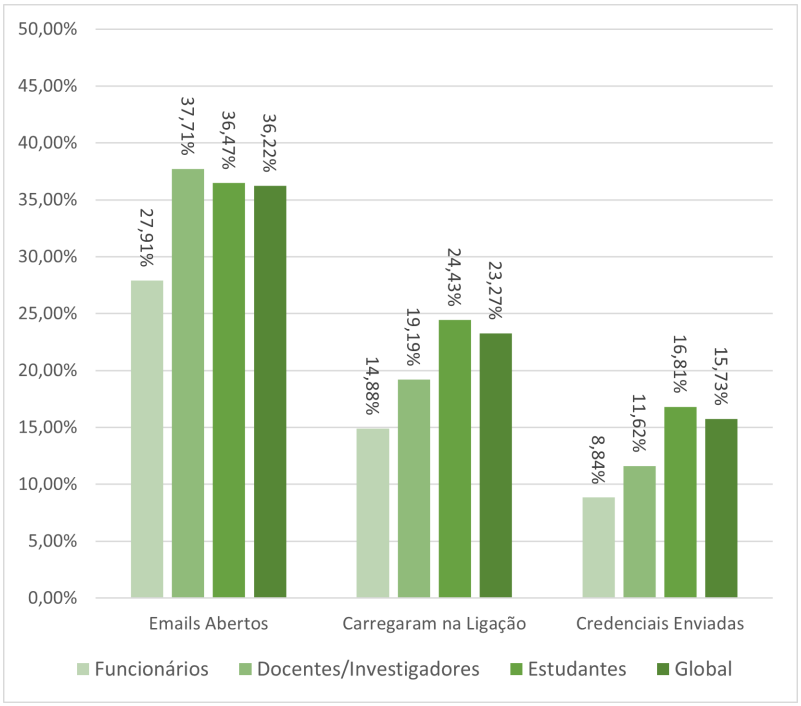

Figura 30: Comparação da frequência relativa (%) dos grupos e do global da primeira campanha.

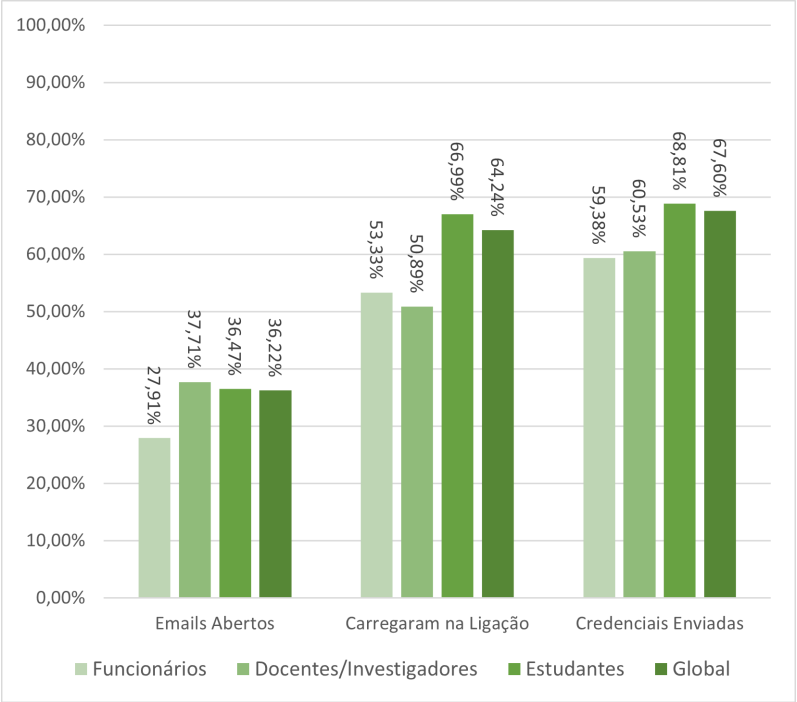

Figura 31: Comparação da frequência relativa (%) em relação ao passo anterior, dos grupos e do global da primeira campanha.

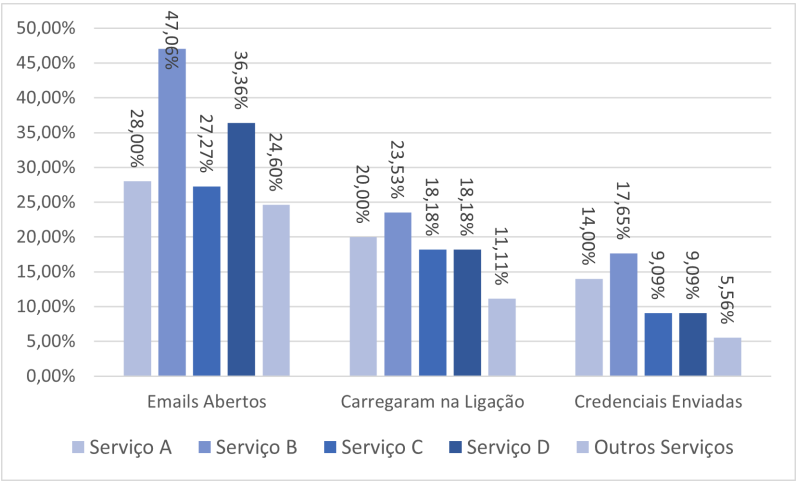

Figura 32: Comparação da frequência relativa (%) dos vários serviços de funcionários da primeira campanha.

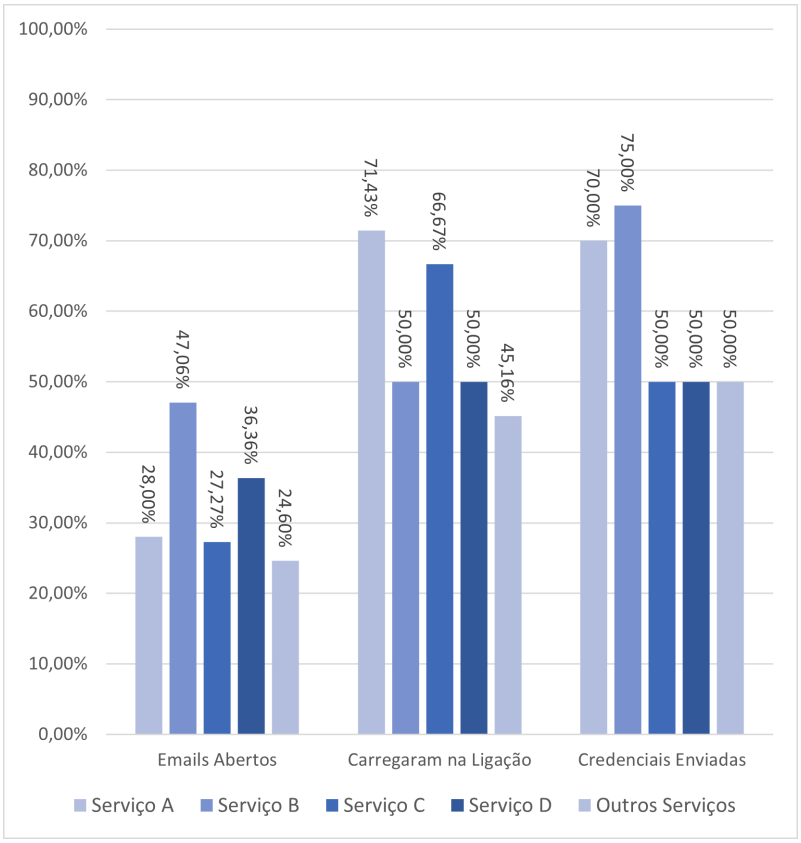

Figura 33: Comparação da frequência relativa (%) em relação ao passo anterior dos funcionários da primeira campanha.

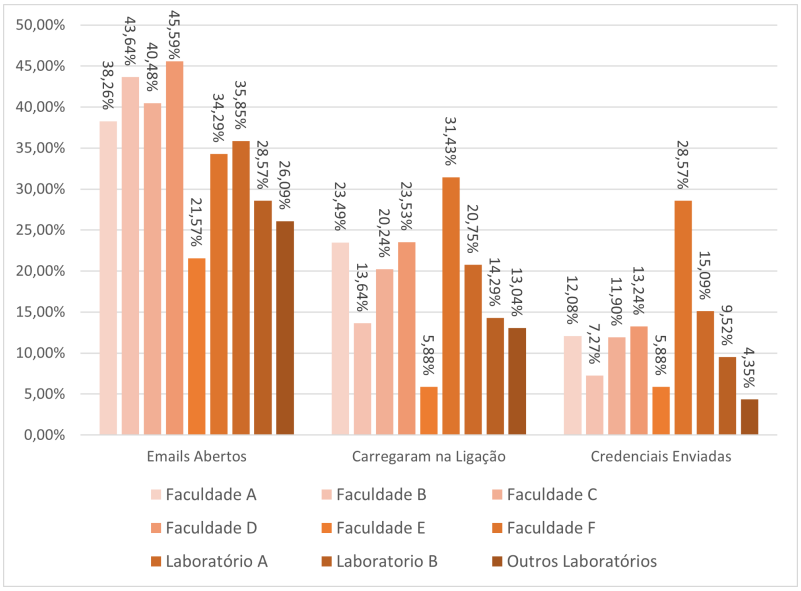

Figura 34: Comparação da frequência relativa (%) das faculdades e laboratórios dos docentes/investigadores da primeira campanha.

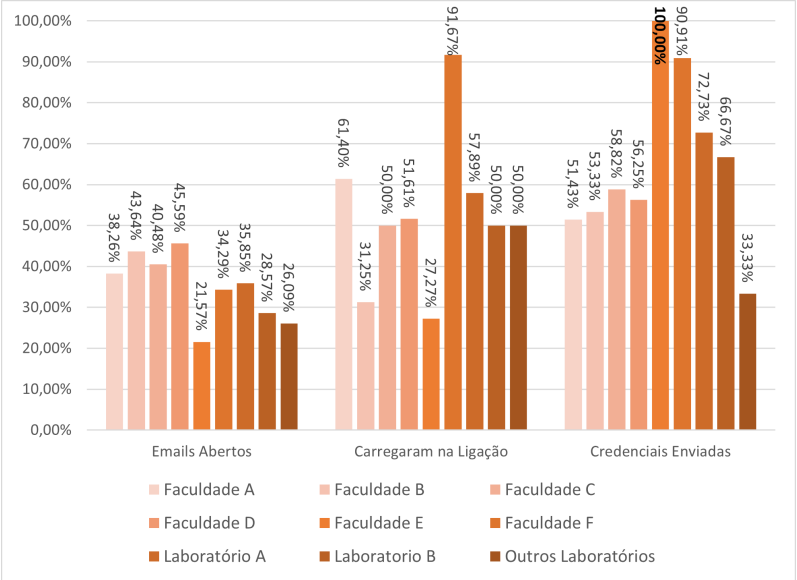

Figura 35: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e laboratórios dos docentes/investigadores da primeira campanha.

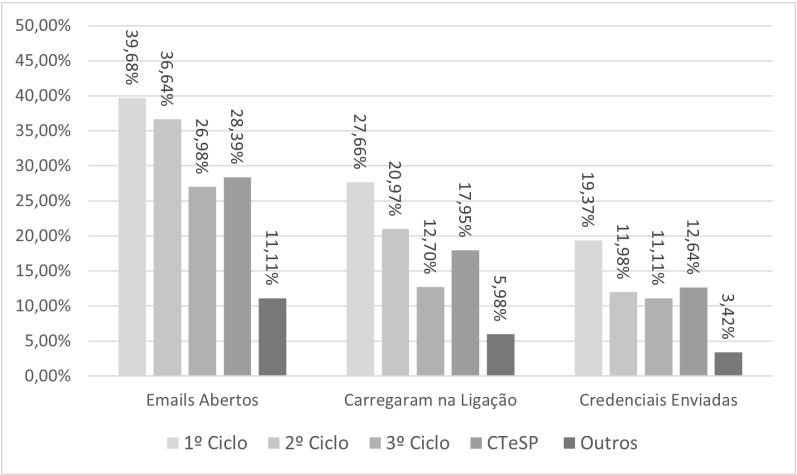

Figura 36: Comparação da frequência relativa (%) dos ciclos dos estudantes da primeira campanha

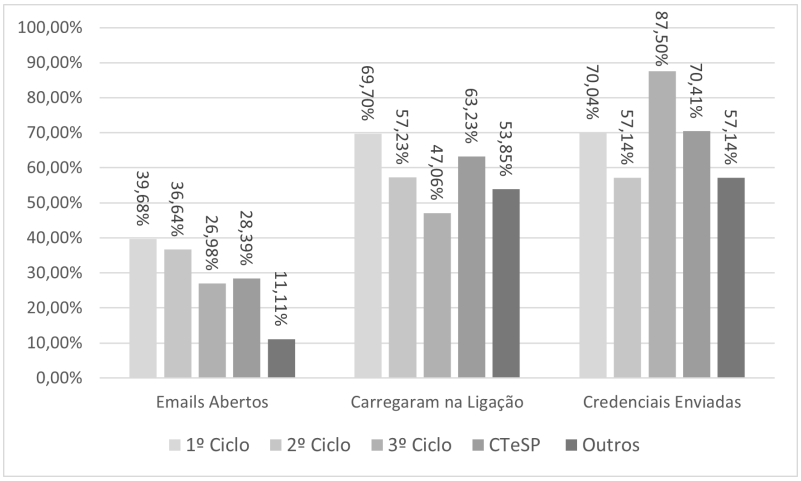

Figura 37: Comparação da frequência relativa (%) em relação ao passo anterior dos ciclos dos estudantes da primeira campanha.

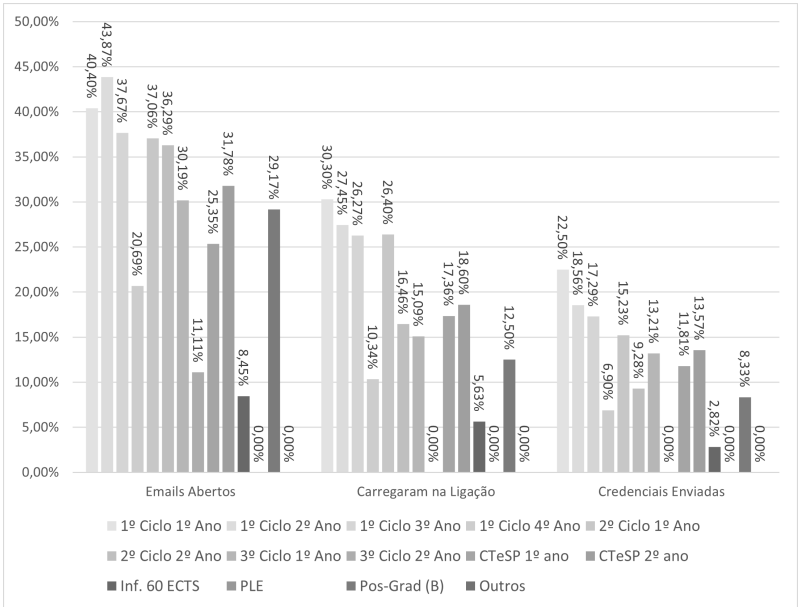

Figura 38: Comparação da frequência relativa (%) dos anos dos estudantes da primeira campanha.

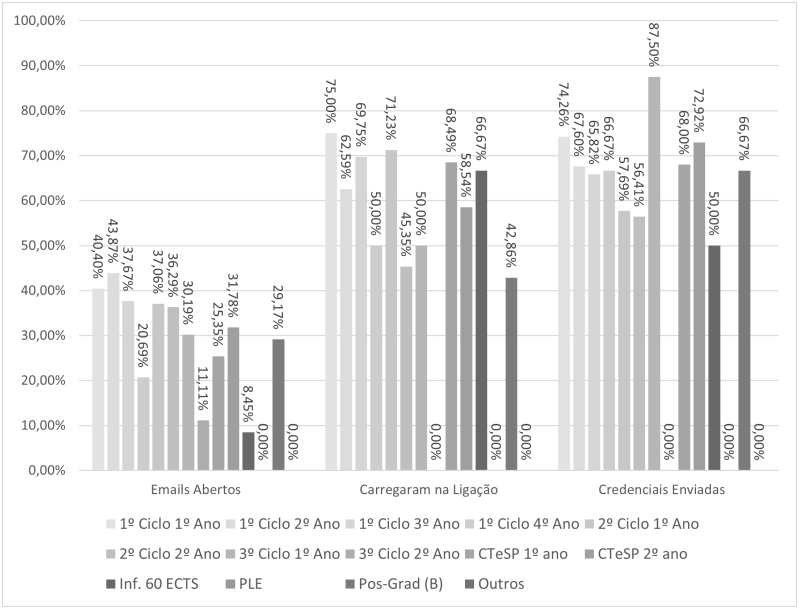

Figura 39: Comparação da frequência relativa (%) em relação ao passo anterior dos anos dos estudantes da primeira campanha.

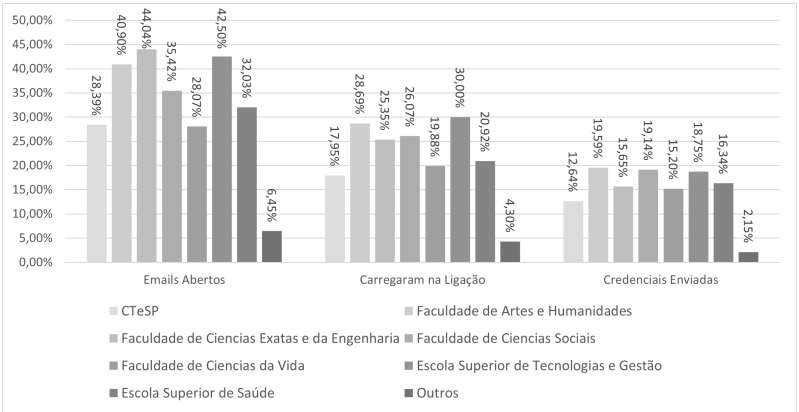

Figura 40: Comparação da frequência relativa (%) das faculdades e escolas dos estudantes da primeira campanha.

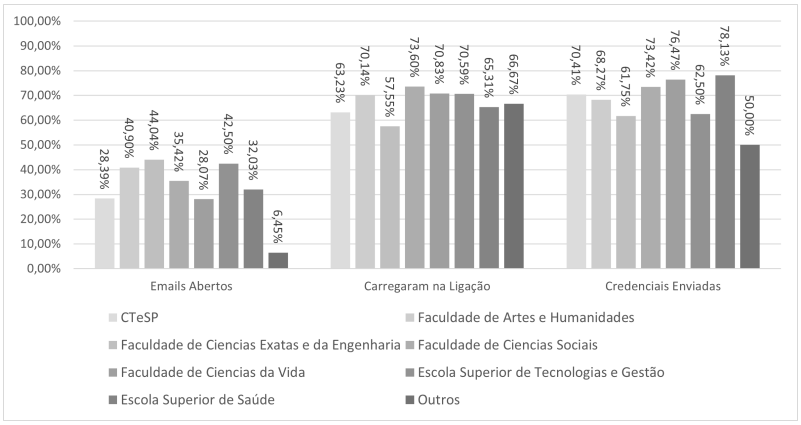

Figura 41: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e escolas dos estudantes da primeira campanha.

O gráfico seguinte mostra o número de pessoas que abriram o e-mail (tenham ou não feito os passos seguintes), em cada dia da duração das campanhas.

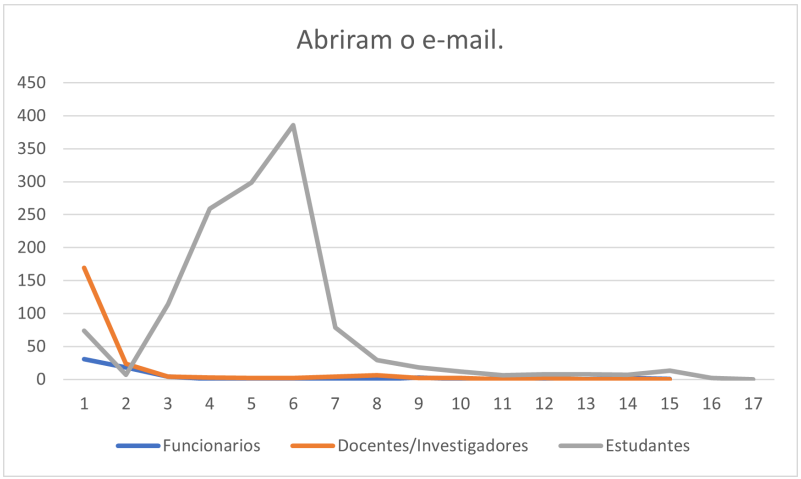

Figura 42: Número por dia de quem abriu o *e-mail* da primeira campanha.

Os três gráficos abaixo mostram o número de pessoas que realizaram cada passo, em cada dia da duração das campanhas.

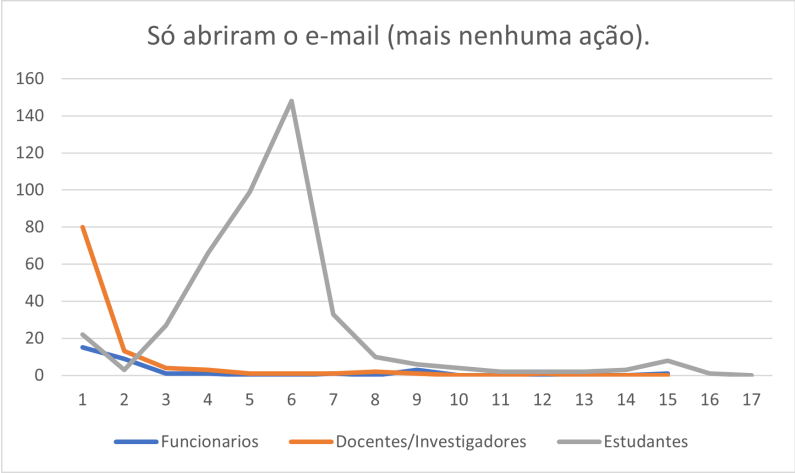

Figura 43: Número por dia de quem só abriu o *e-mail* da primeira campanha.

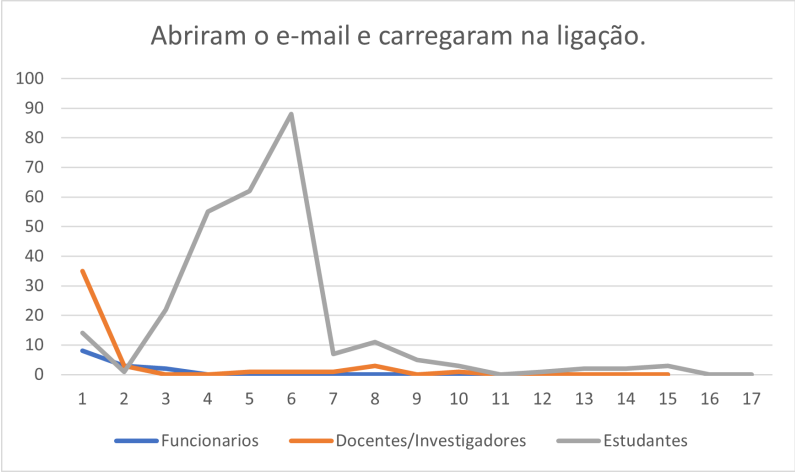

Figura 44: Número por dia de quem abriu o *e-mail* e carregou na ligação da primeira campanha.

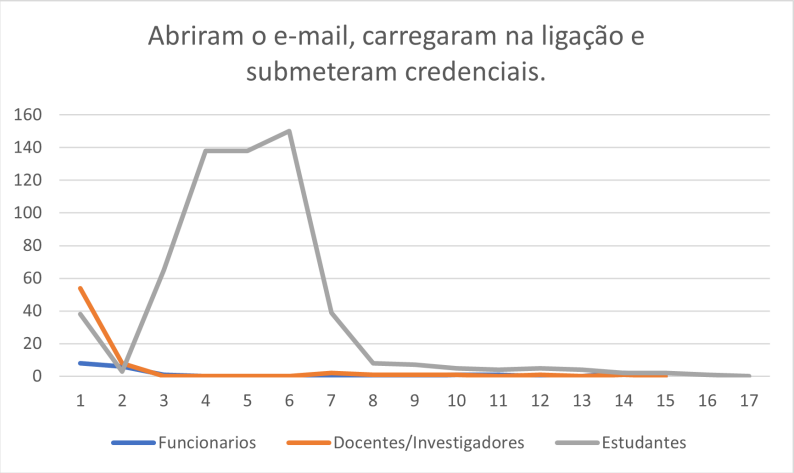

Figura 45: Número por dia de quem abriu o *e-mail*, carregou na ligação e submeteu credenciais da primeira campanha.

Resultados da Segunda Campanha

Nesta secção também são apresentados os gráficos e tabelas em relação aos membros que receberam o *e-mail* informativo.

Tabela 23: Resultados do envio do *e-mail* informativo.

Grupo	*E-mails* Enviados	*E-mails* Abertos	Frequência Relativa (%)
Global	1031	540	52,37%
Funcionários	32	15	46,88%
Docentes/Investigadores	114	64	56,14%
Estudantes	885	461	52,09%

Tabela 24: Resultados globais da segunda campanha.

E-mails Enviados	E-mails Abertos	Carregaram na Ligação
4458	1876	934
-	42,08%	20,95%
-	-	49,79%

Tabela 25: Resultados globais da segunda campanha de quem abriu o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
540	444	215
-	82,22%	39,81%
-	-	48,42%

Tabela 26: Resultados dos funcionários da segunda campanha.

E-mails Enviados	E-mails Abertos	Carregaram na Ligação
215	91	72
-	42,33%	33,49%
-	-	79,12%

Tabela 27: Resultados dos funcionários da segunda campanha que abriram o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
15	14	13
-	93,33%	86,64%
-	-	92,86%

Tabela 28: Resultados dos docentes/investigadores da segunda campanha

E-mails Enviados	E-mails Abertos	Carregaram na Ligação
594	261	152
-	43,94%	25,59%
-	-	58,24%

Tabela 29: Resultados dos docentes/investigadores da segunda campanha que abriram o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
64	47	34
-	73,44%	53,13%
-	-	72,34%

Tabela 30: Resultados dos estudantes da segunda campanha

E-mails Enviados	E-mails Abertos	Carregaram na Ligação
3649	1524	710
-	41,76%	19,46%
-	-	46,59%

Tabela 31: Resultados dos estudantes da segunda campanha que abriram o *e-mail* informativo.

E-mails Enviados	*E-mails* Abertos	Carregaram na Ligação
461	383	159
-	83,08%	34,49%
-	-	41,51%

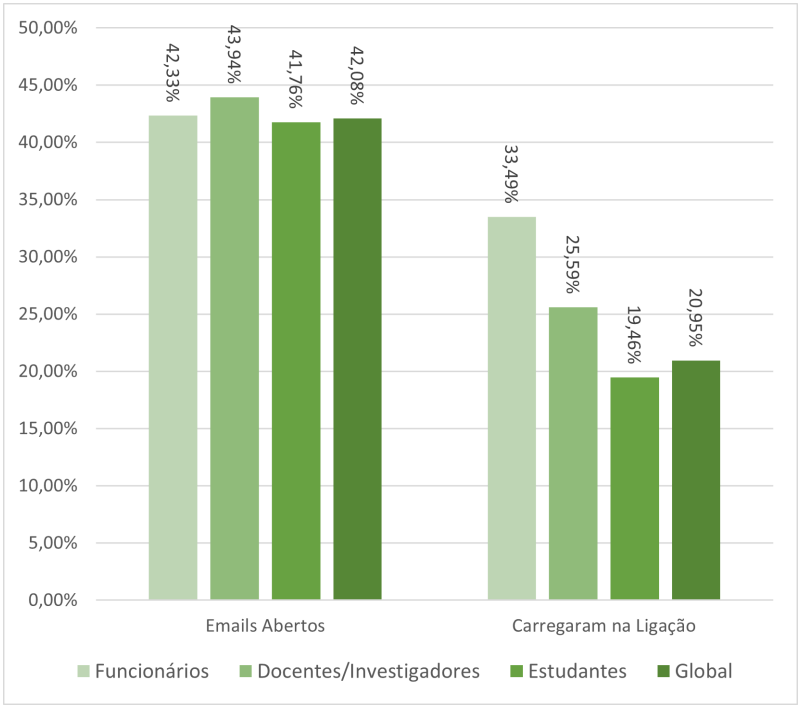

Figura 46: Comparação da frequência relativa (%) dos grupos e do global da segunda campanha.

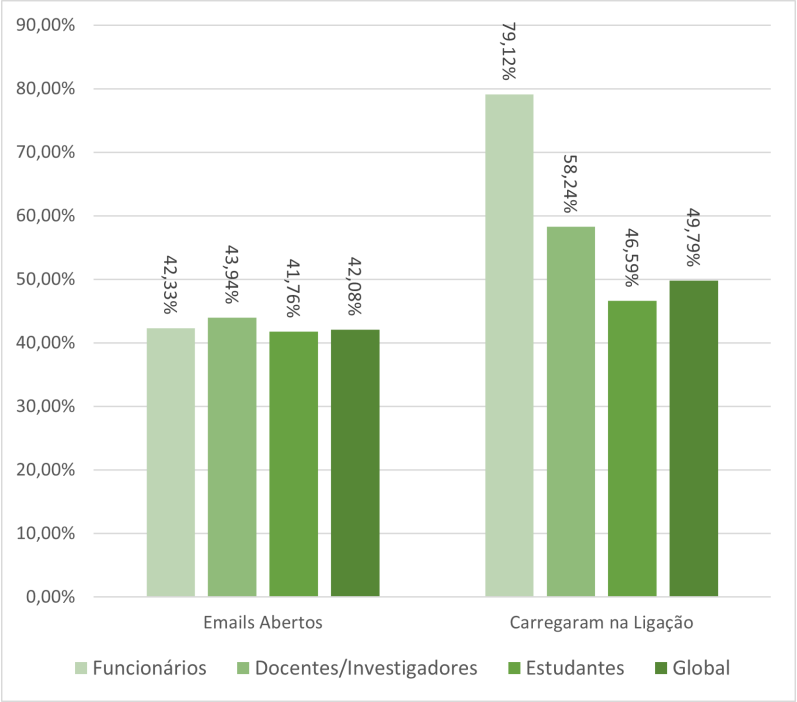

Figura 47: Comparação da frequência relativa (%) dos grupos e do global da segunda campanha.

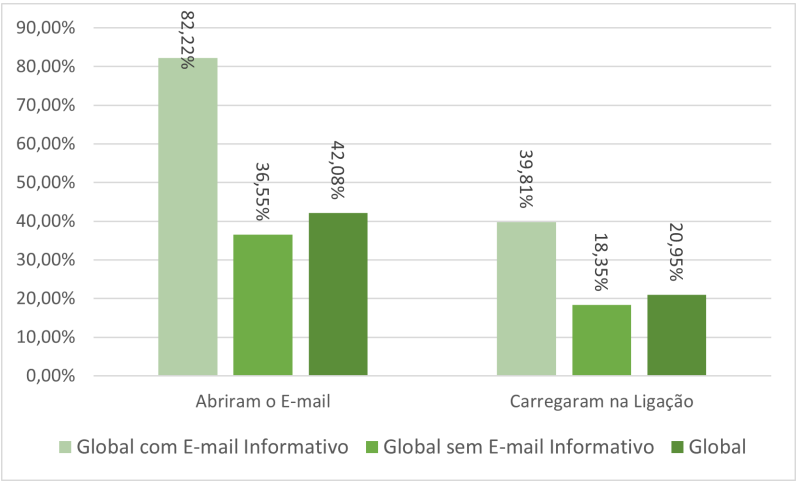

Figura 48: Comparação global com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

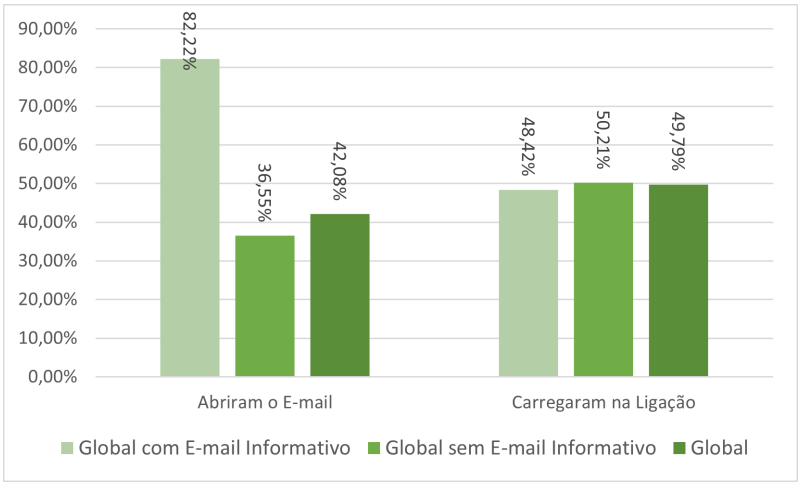

Figura 49: Comparação global com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

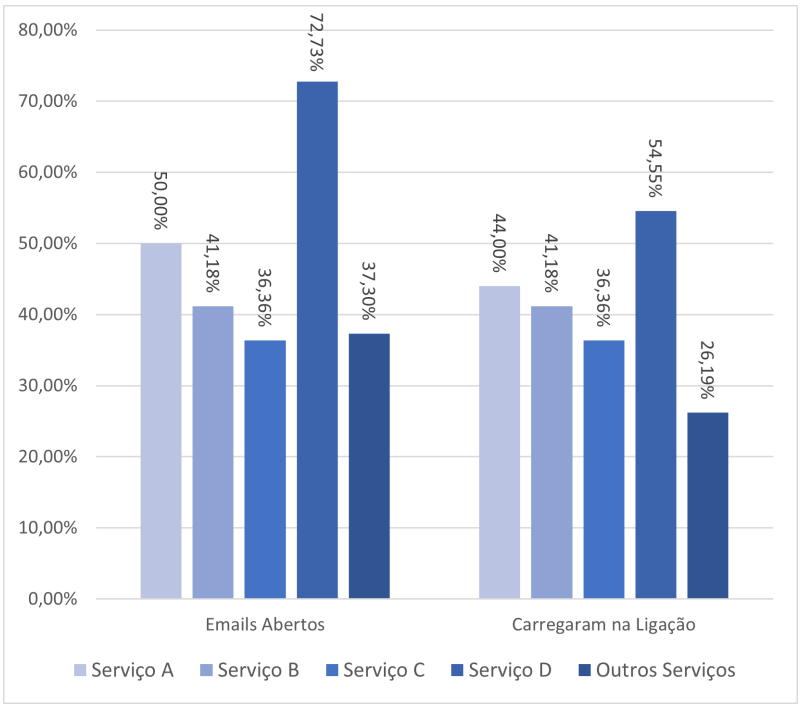

Figura 50: Comparação da frequência relativa (%) dos vários serviços de funcionários da segunda campanha.

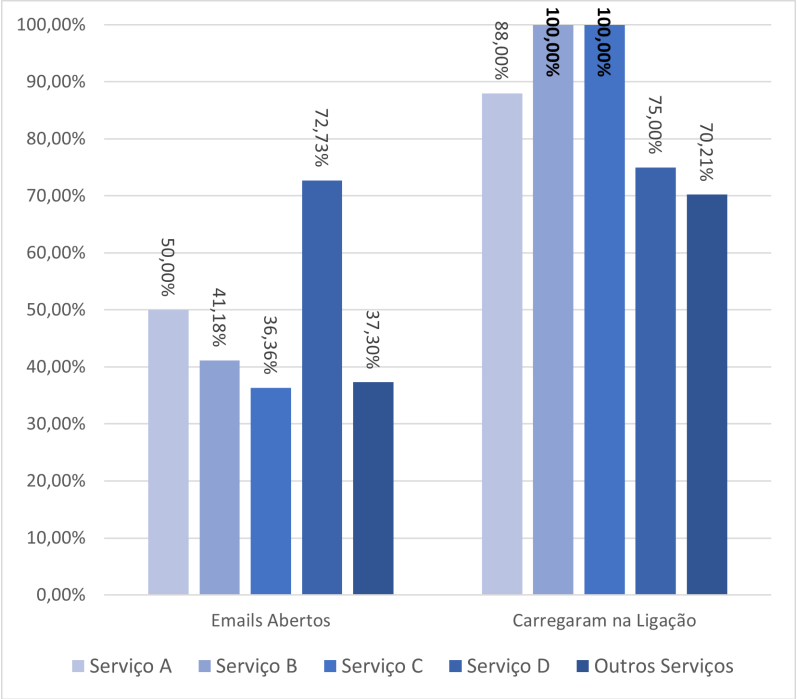

Figura 51: Comparação da frequência relativa (%) em relação ao passo anterior dos funcionários da segunda campanha.

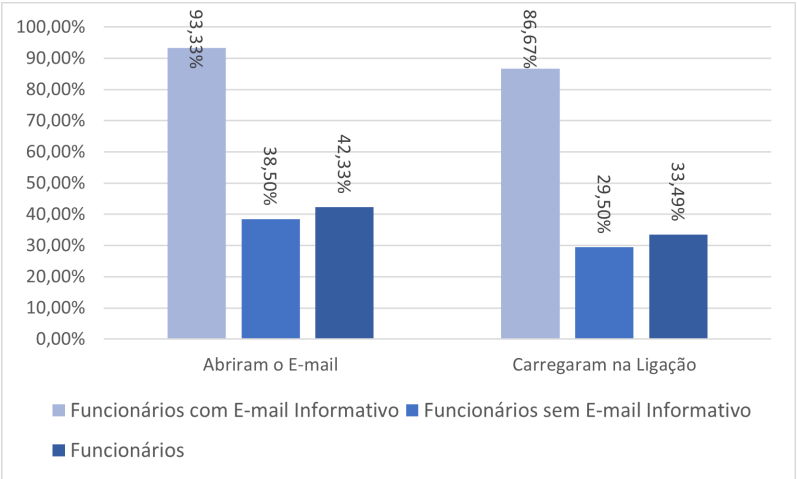

Figura 52: Comparação de funcionários com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

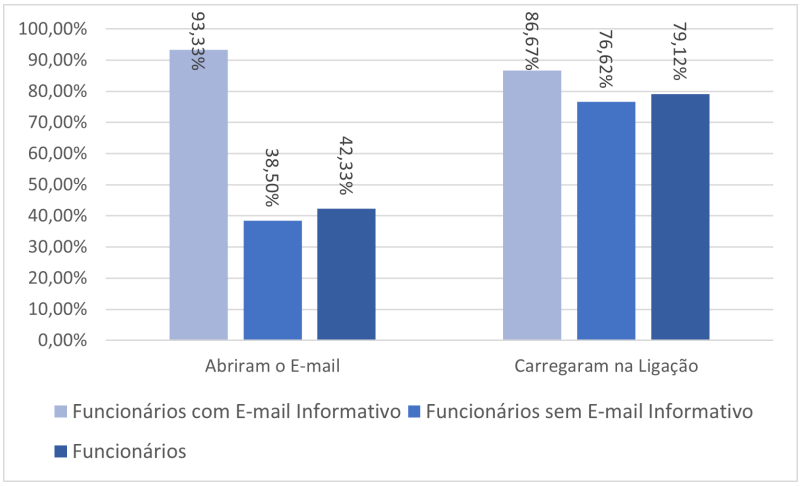

Figura 53: Comparação de funcionários com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

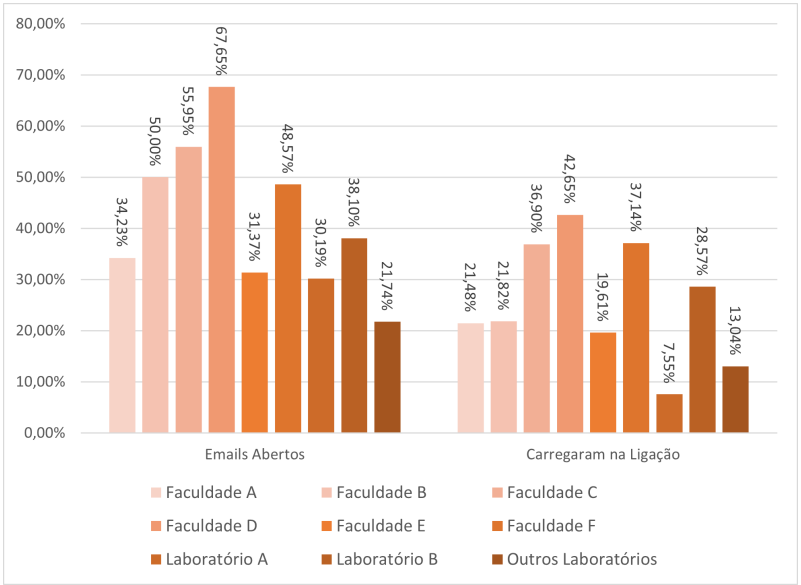

Figura 54: Comparação da frequência relativa (%) das faculdades e laboratórios dos docentes/investigadores da segunda campanha.

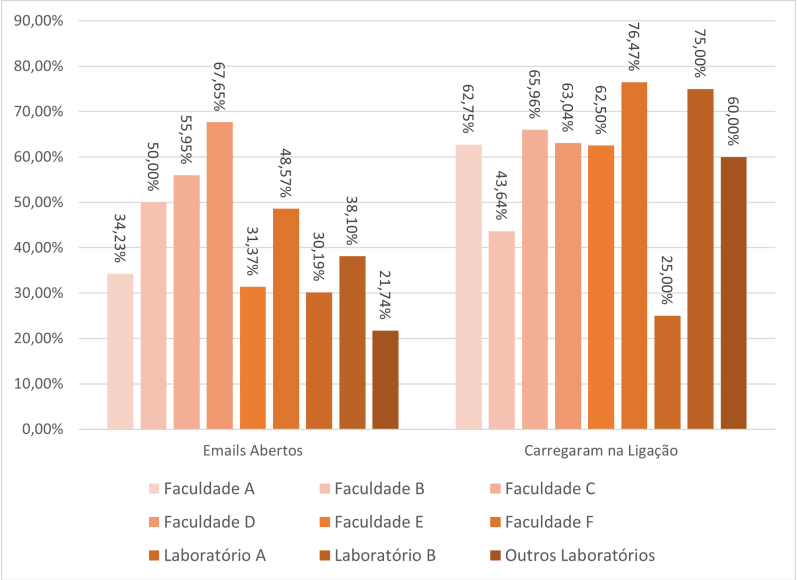

Figura 55: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e laboratórios dos docentes/investigadores da segunda campanha.

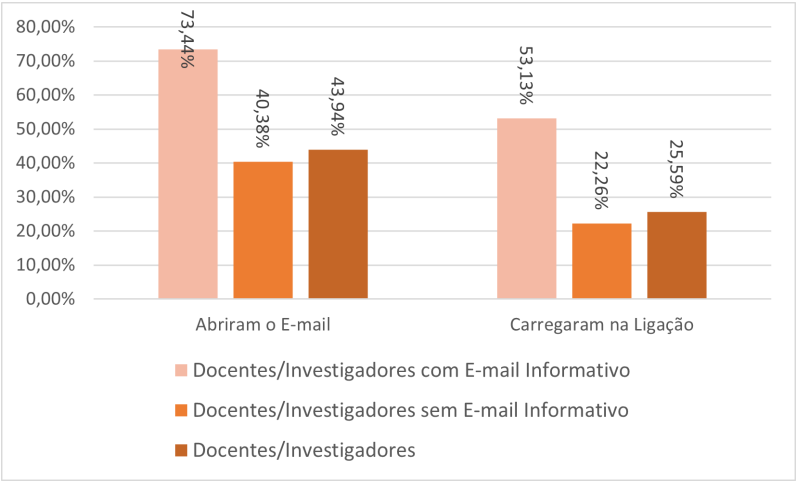

Figura 56: Comparação docentes/investigadores com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

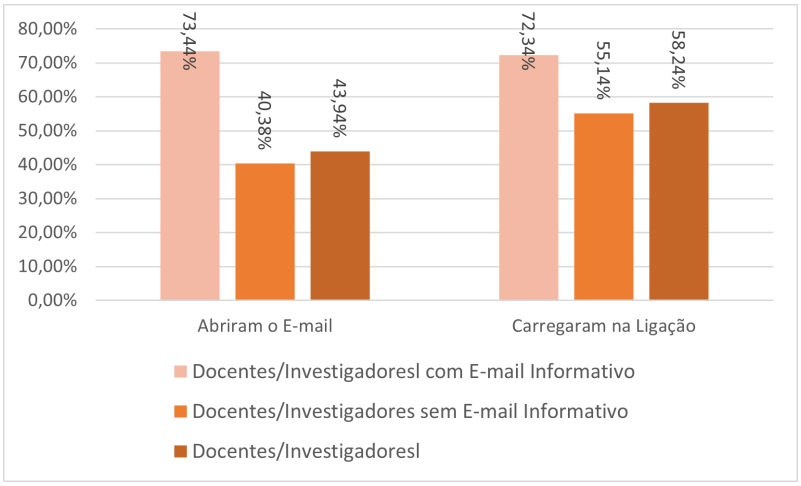

Figura 57: Comparação docentes/investigadores com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

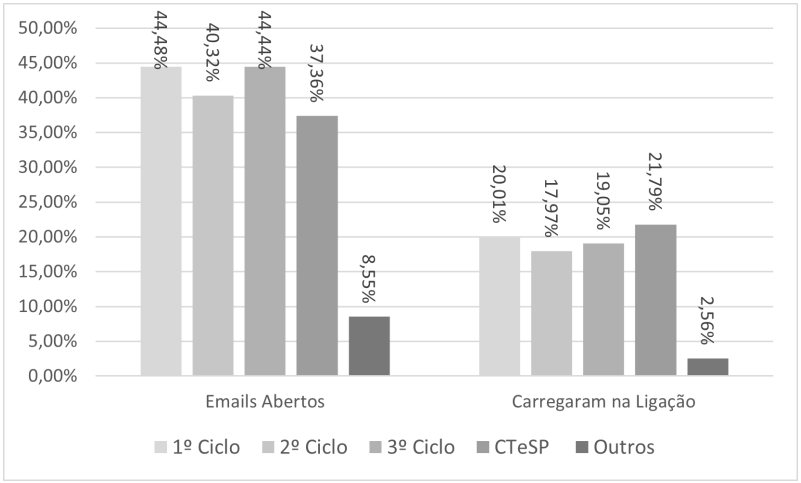

Figura 58: Comparação da frequência relativa (%) das faculdades e laboratórios dos docentes/investigadores da segunda campanha.

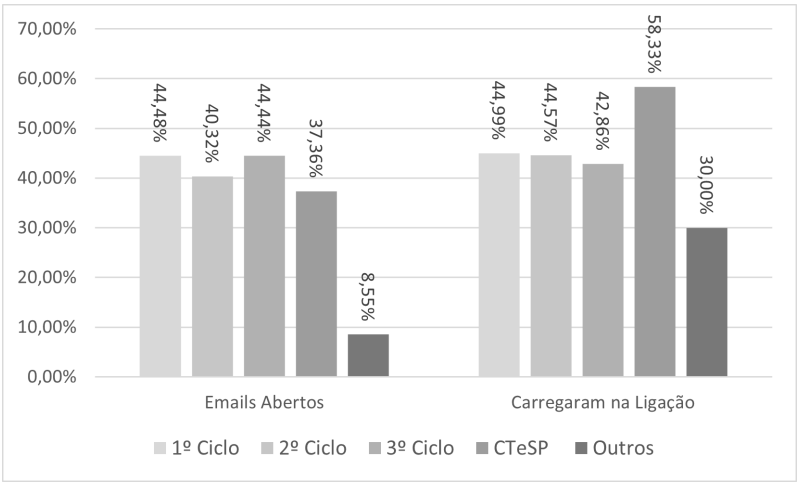

Figura 59: Comparação da frequência relativa (%) em relação ao passo anterior dos ciclos dos estudantes da segunda campanha.

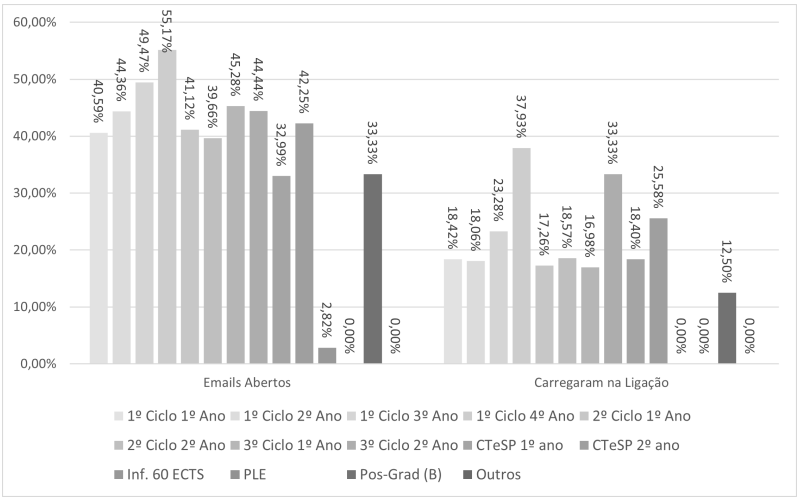

Figura 60: Comparação da frequência relativa (%) dos anos dos estudantes da segunda campanha.

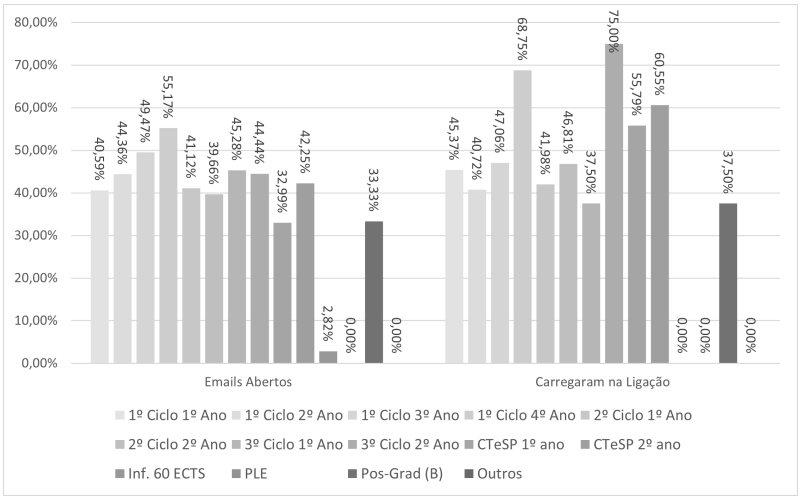

Figura 61: Comparação da frequência relativa (%) em relação ao passo anterior dos anos dos estudantes da segunda campanha.

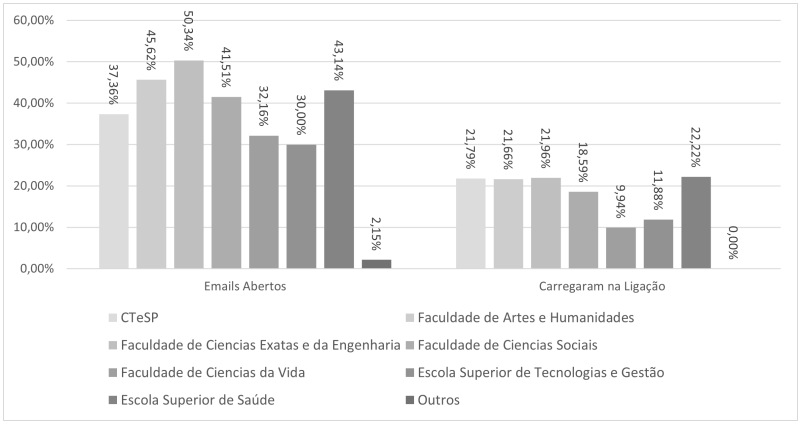

Figura 62: Comparação da frequência relativa (%) das faculdades e escolas dos estudantes da segunda campanha.

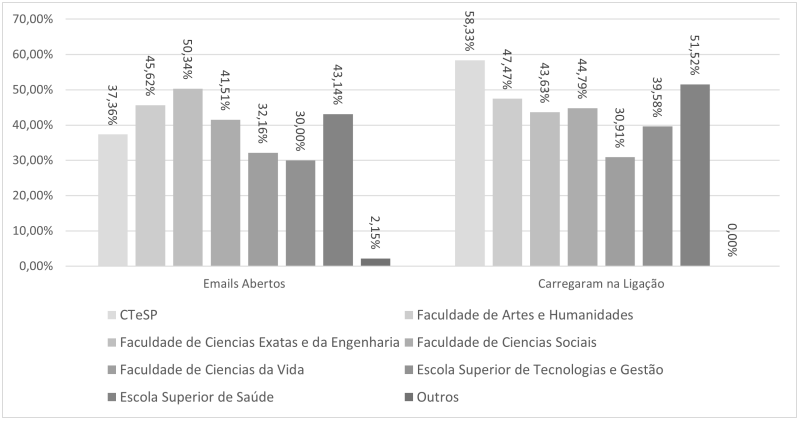

Figura 63: Comparação da frequência relativa (%) em relação ao passo anterior das faculdades e escolas dos estudantes da segunda campanha.

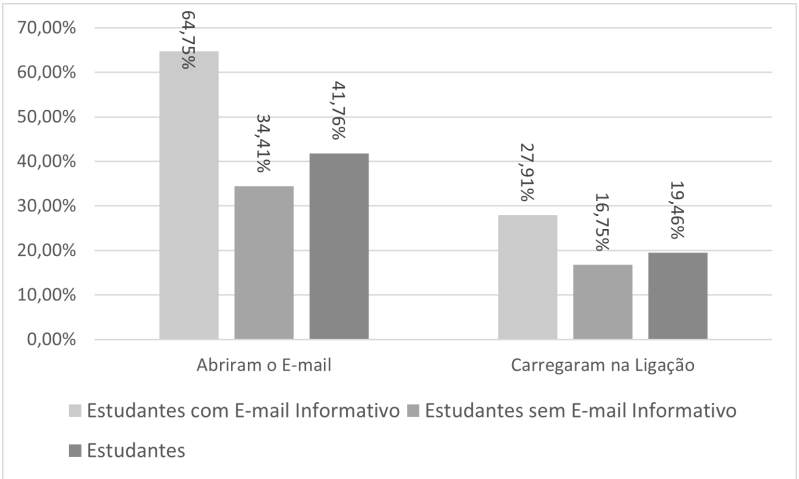

Figura 64: Comparação de estudantes com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

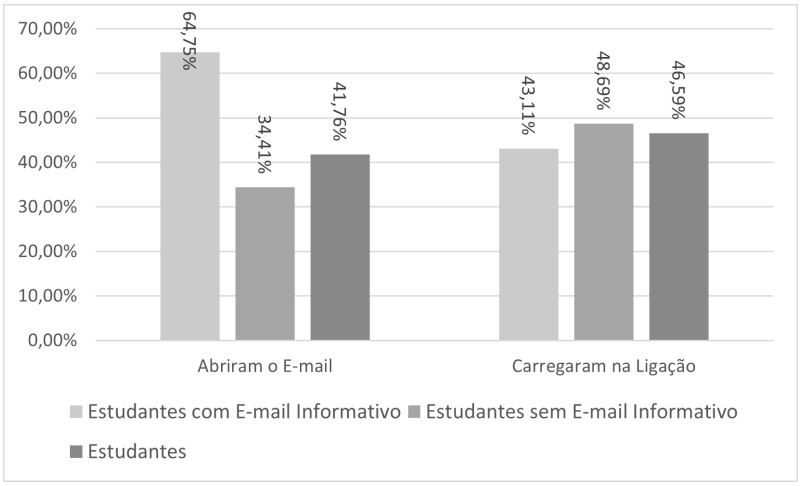

Figura 65: Comparação de estudantes com e sem *e-mail* informativo, usando a frequência relativa (%) em relação ao passo anterior.

O gráfico seguinte mostra o número de pessoas que abriram o e-mail (tenham ou não feito os passos seguintes), em cada dia da duração das campanhas.

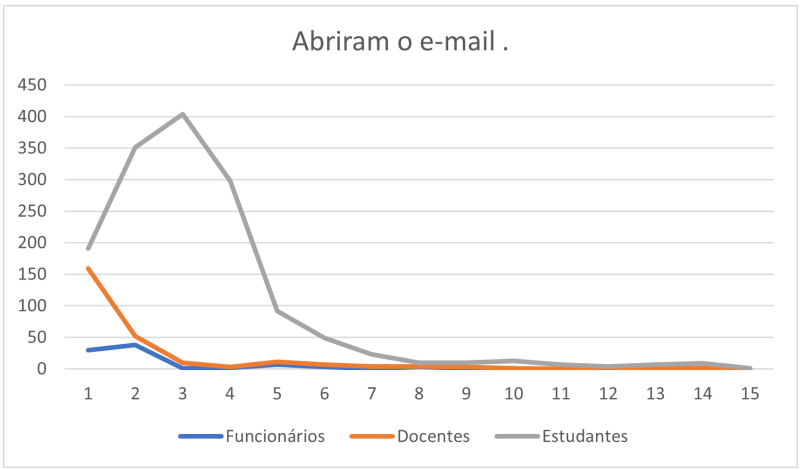

Figura 66: Número por dia de quem abriu o *e-mail* da primeira campanha.

Os três gráficos abaixo mostram o número de pessoas que realizaram cada passo, em cada dia da duração das campanhas.

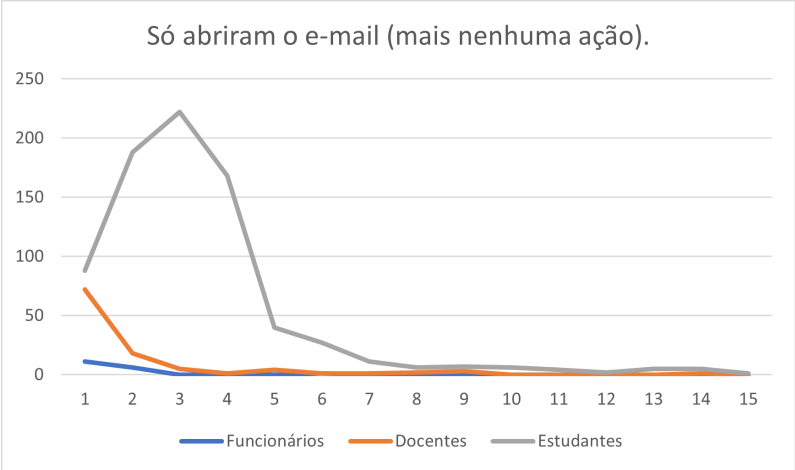

Figura 67: Número por dia de quem só abriu o *e-mail* da segunda campanha.

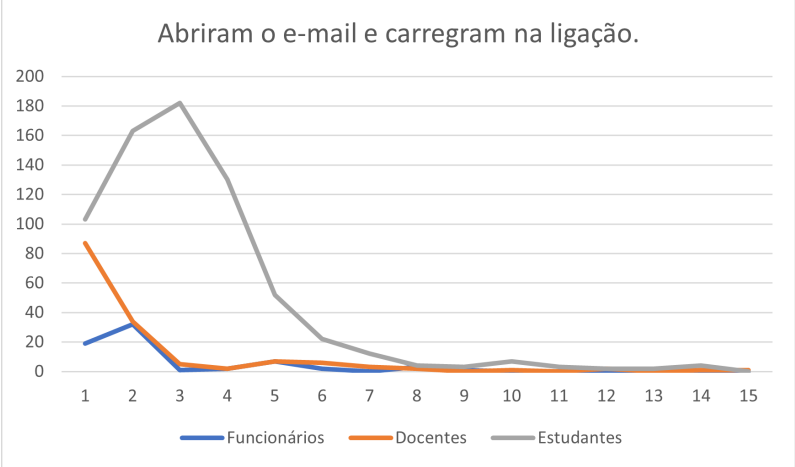

Figura 68: Número por dia de quem abriu o *e-mail* e carregou na ligação da segunda campanha.

Anexos B - Interface do *Gophish*

Para poder dar inicio a uma campanha no Gophish é necessário configurar o perfil de envio, o grupo a quem a campanha é dirigida, o modelo do *e-mail* a ser enviado e a página à qual os alvos vão ser redirecionados.

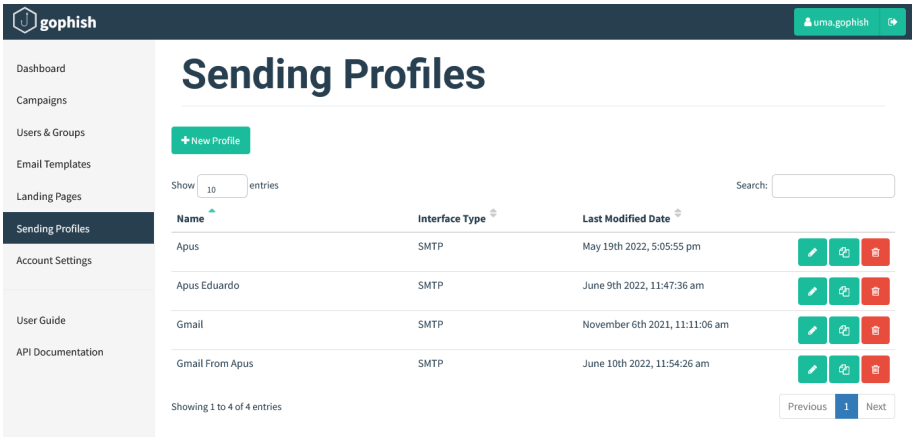

Figura 69: Painel de consulta de perfis de envio.

Ao criar um perfil de envio (Figura 69) é necessário conectar a uma conta de *e-mail* pré-existente e a um servidor de SMTP. A conta Gmail criada para este projeto (Serviços de Apoio) foi conectada e os *e-mails* foram enviados através do servidor *SMTP* da Google (Figura 70).

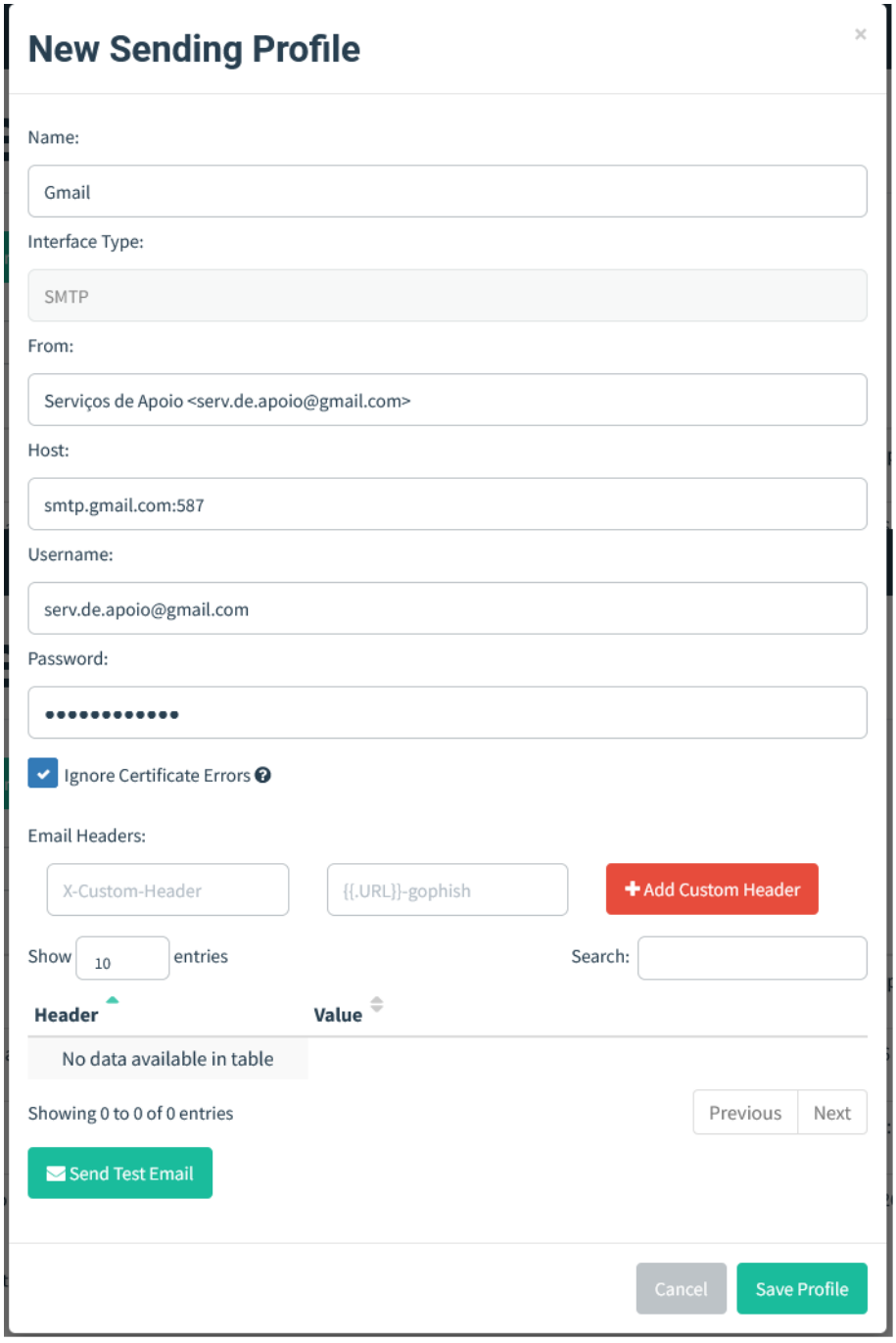

Figura 70: Menu para conectar conta para enviar *e-mails*

Os grupos (Figura 71) são compostos por utilizadores, a quem será enviado o *e-mail*, e não tem limite de elementos. Os grupos principais para este projeto foram funcionários, docentes/investigadores e estudantes.

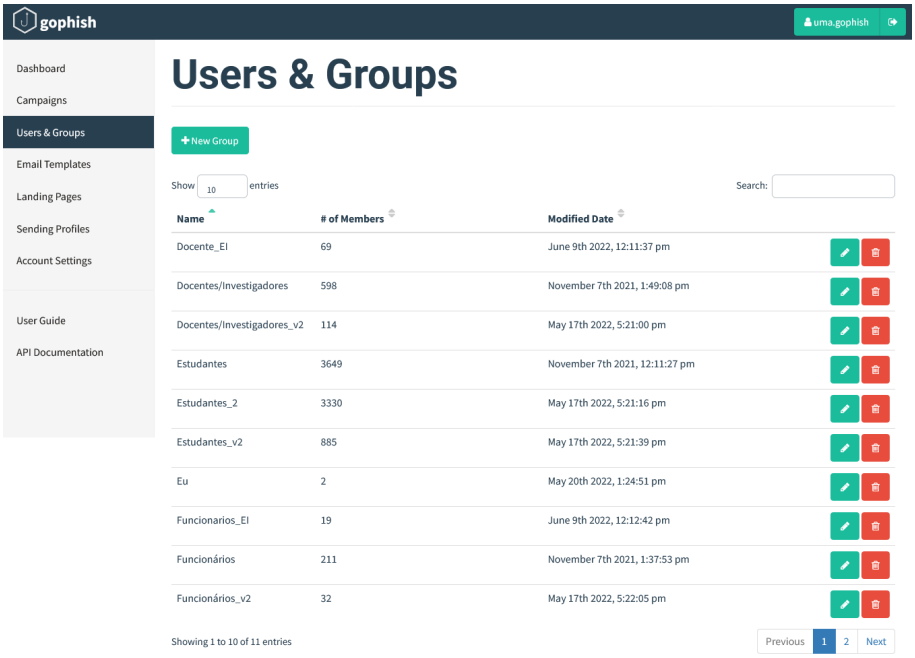

Figura 71: Painel de consulta de utilizadores e grupos.

A identificação de cada utilizador é feita com quatro campos, primeiro nome, último nome, *e-mail* e cargo (Figura 72). Os *e-emails* usados durante a criação de grupos foram os institucionais da UMa, e o cargo serviu para identificar o serviço, a faculdade e o curso.

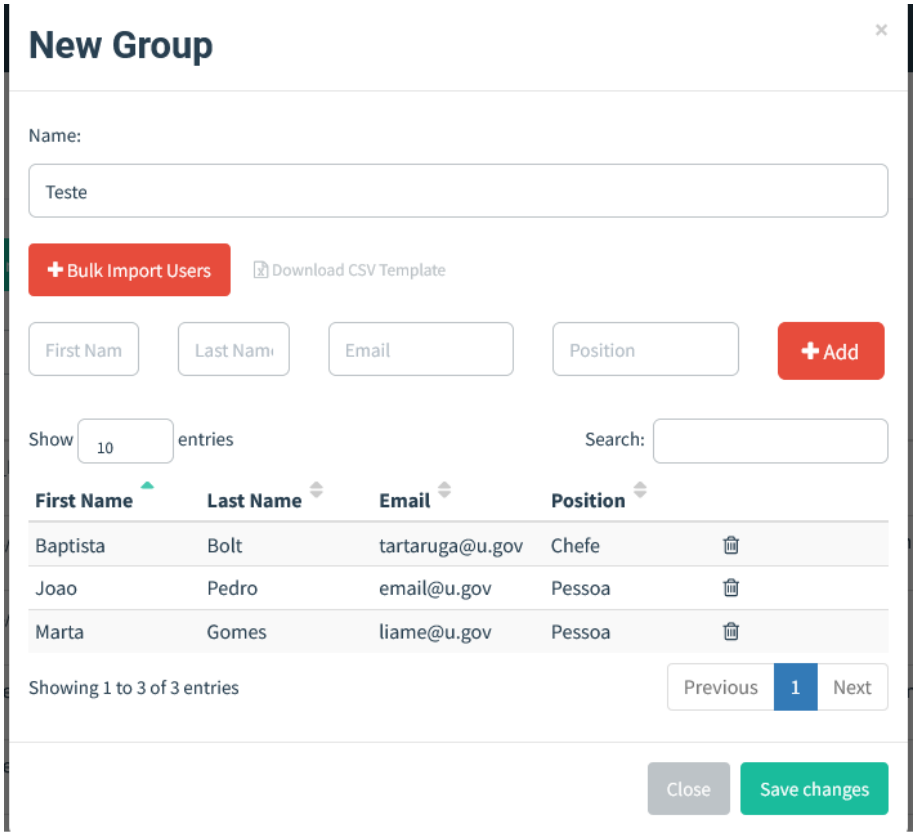

Figura 72: Menu para registar utilizadores e criar grupos.

Cada campanha precisa de um modelo de *e-mail* (Figura 73), que será enviado a todos os elementos do grupo selecionado para a campanha.

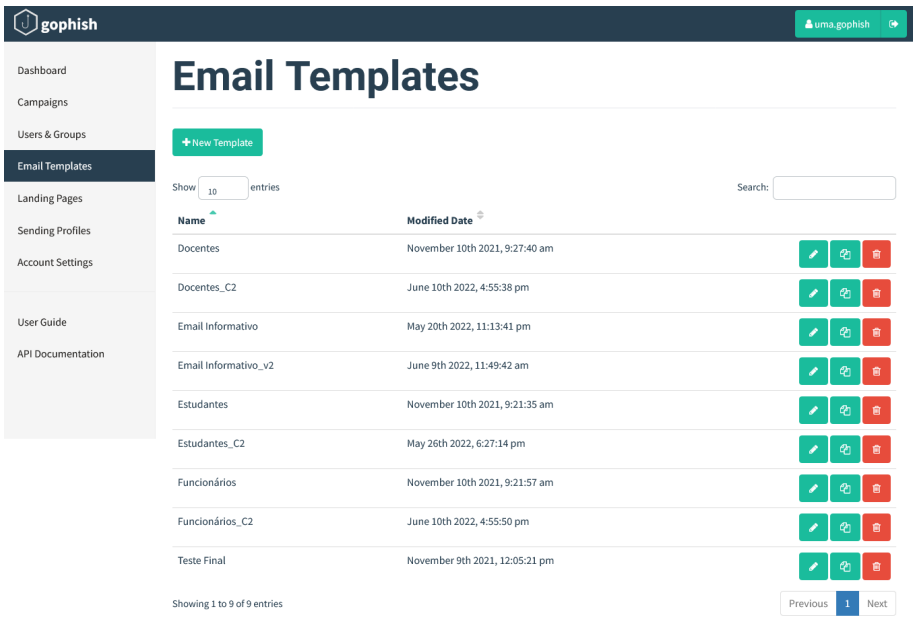

Figura 73: Painel de consulta de modelos de *e-mail*.

O *e-mail* é composto por assunto e pela mensagem, havendo a opção de adicionar uma *Tracking Image*, para monitorizar quando os *e-mails* são abertos (Figura 74).

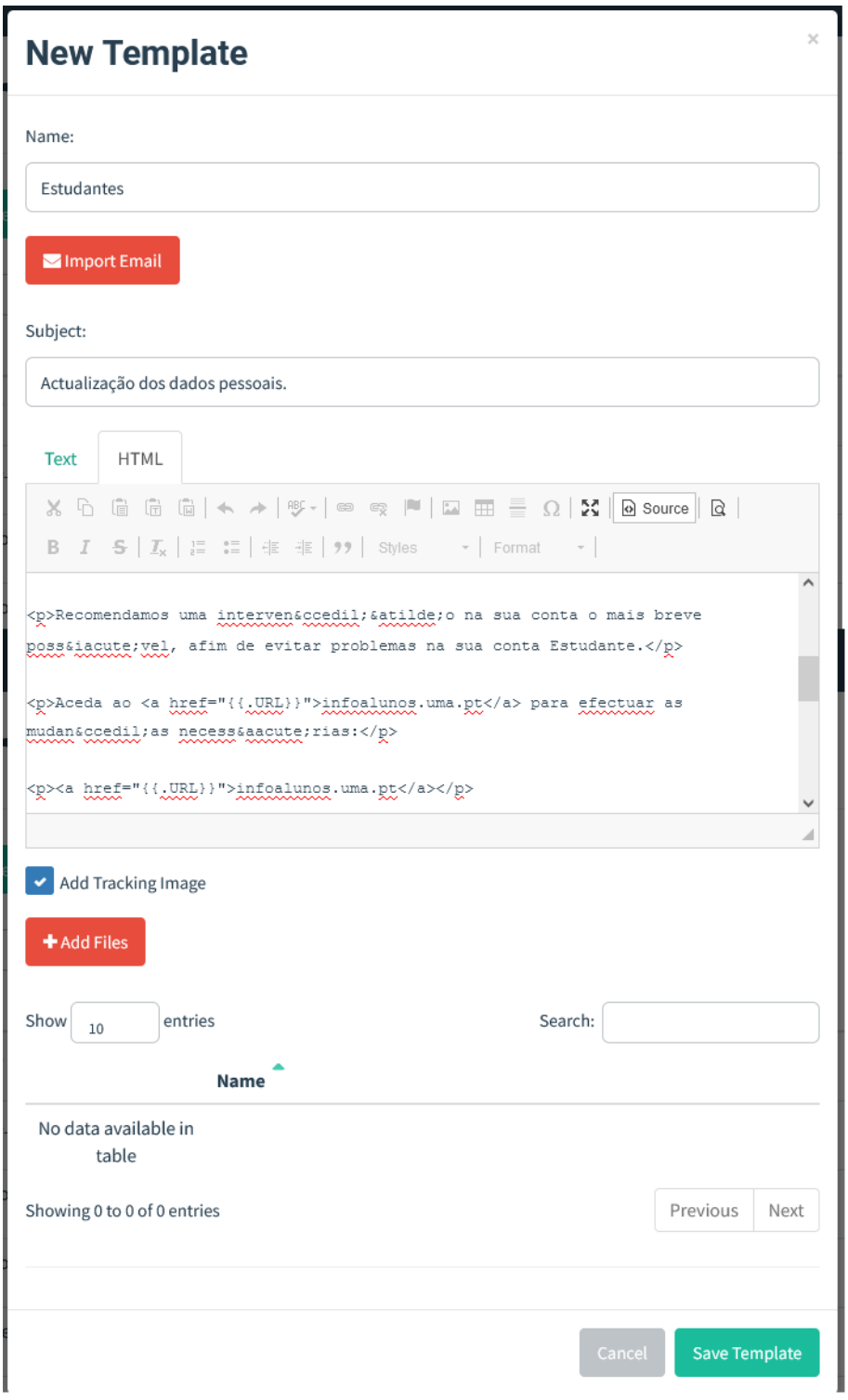

Figura 74: Menu para criar modelo de *e-mail*.

Uma página de redirecionamento pode ou não fazer parte de uma campanha. Para ambos os ataques de *phishing* foi criada uma (Figura 75), para monitorizar quem carregava na ligação falsa.

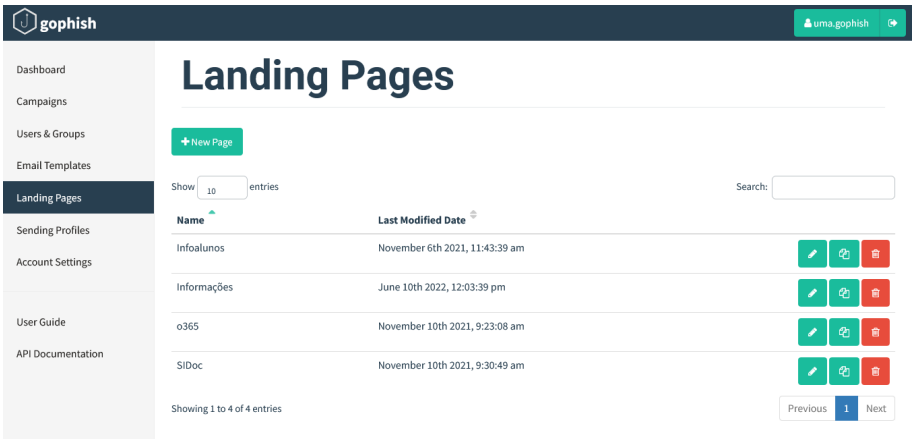

Figura 75: Painel de consulta das páginas de redirecionamento.

A criação da página (Figura 76) era simplificada, pois podia ser feita ao copiar um endereço, através do botão 'Import Site', e o Gophish criava uma copia dessa página automaticamente.

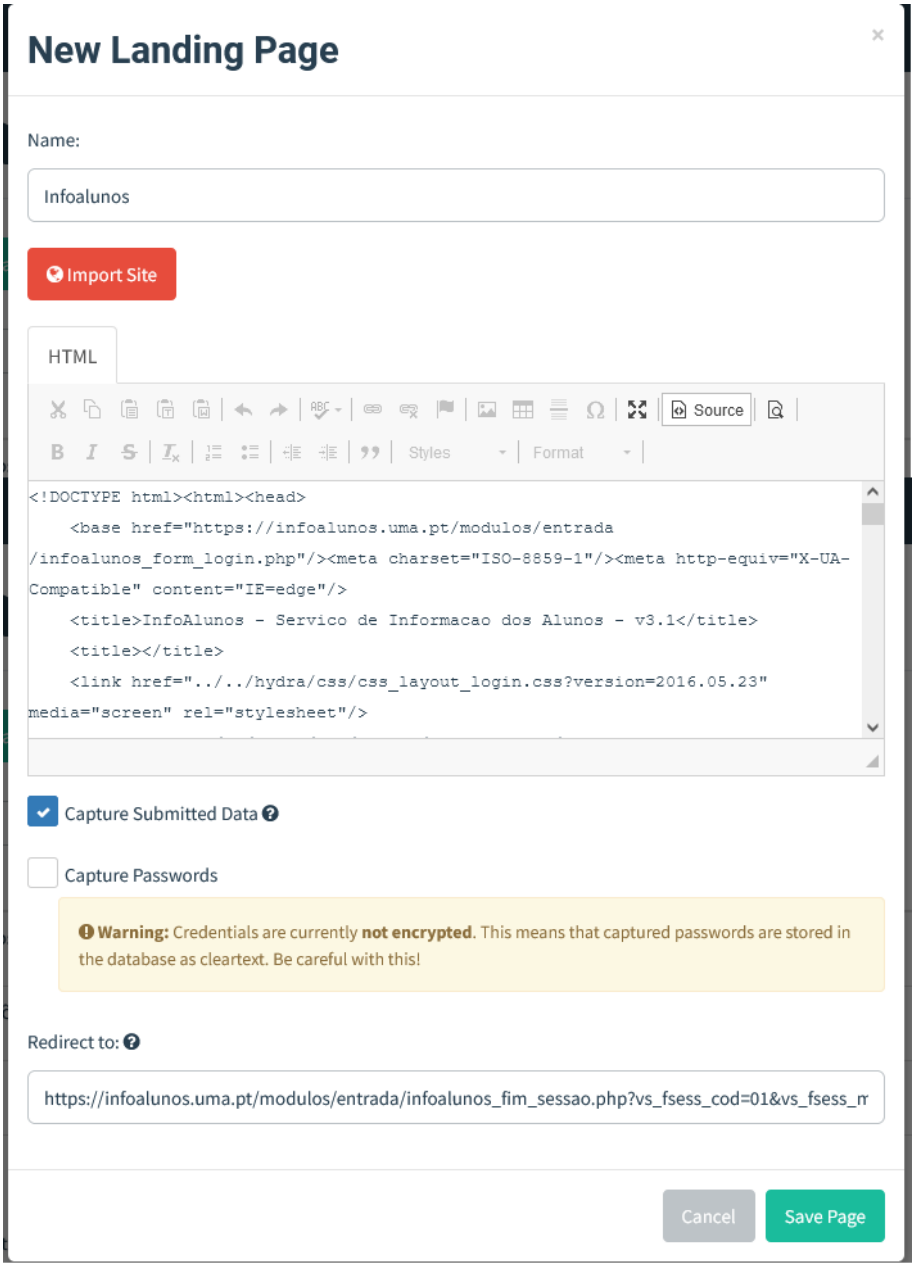

Figura 76: Menu para criar página de redirecionamento.

Após configurar tudo o que é necessário pode ser criada a campanha de *phishing* (Figura 77).

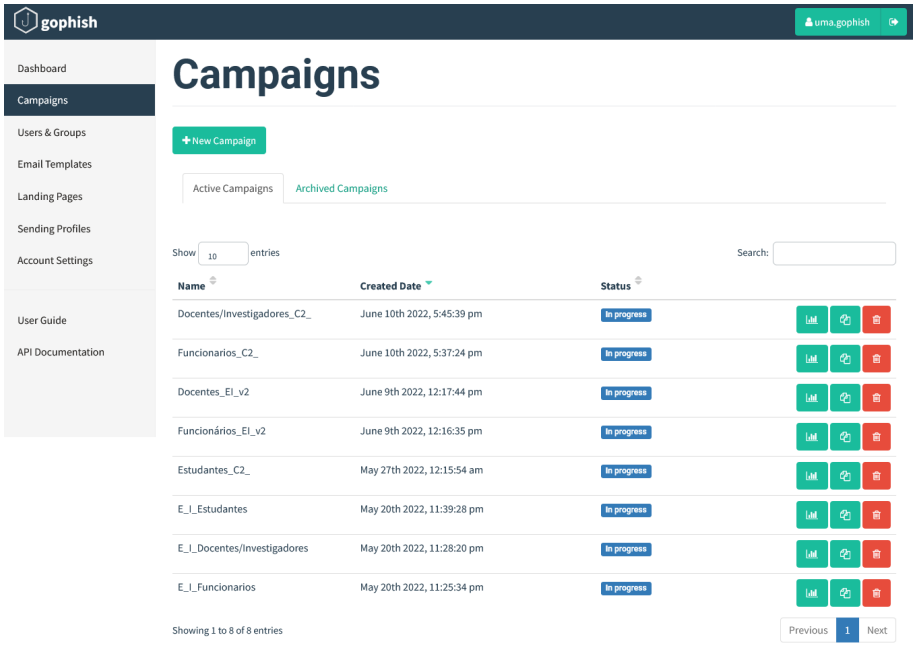

Figura 77: Painel de consulta das campanhas.

Em conjunto com a seleção do modelo de *e-mail*, da página de redirecionamento, do perfil de envio e do grupo, é necessário escolher a data para começar os envios e a data até quando estes envios são feitos, desta forma o Gophish envia os *e-mails* ao longo do tempo de forma uniforme (Figura 78). O URL é o endereço do servidor que está a escuta da parte do Gophish para registar as ações dos utilizadores.

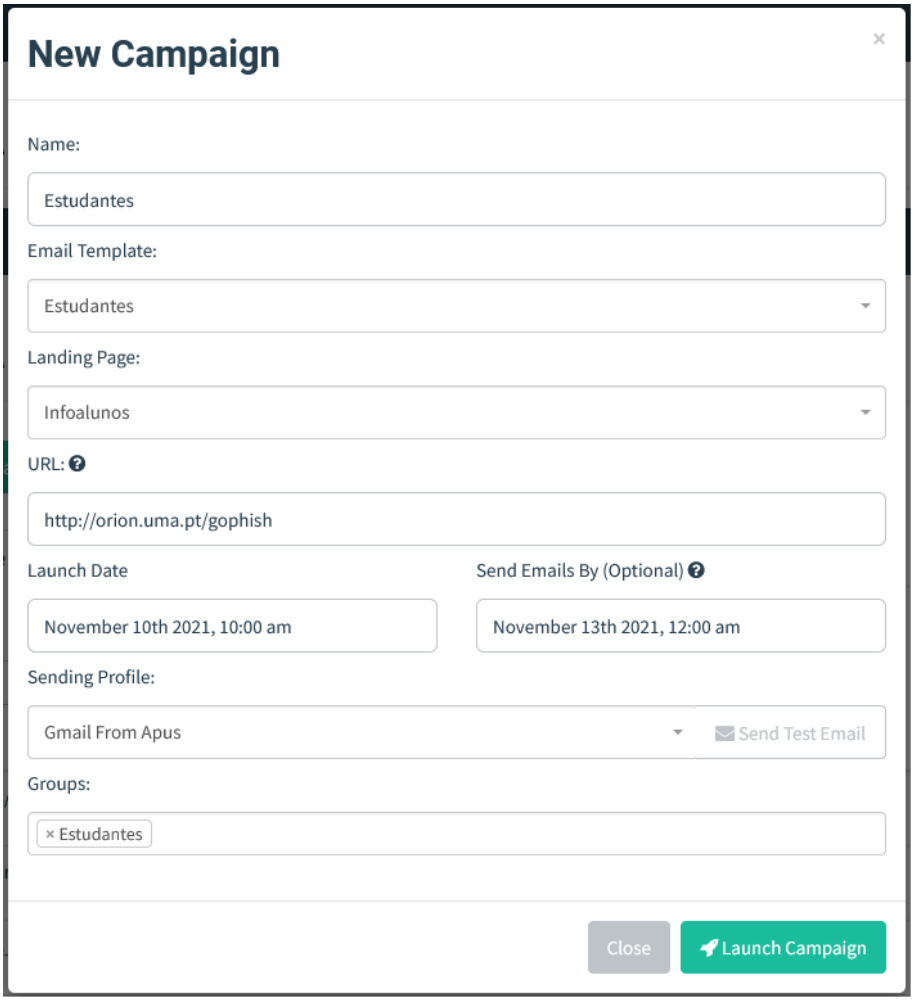

Figura 78: Menu para criar campanha.

Anexos C - Páginas de Alerta

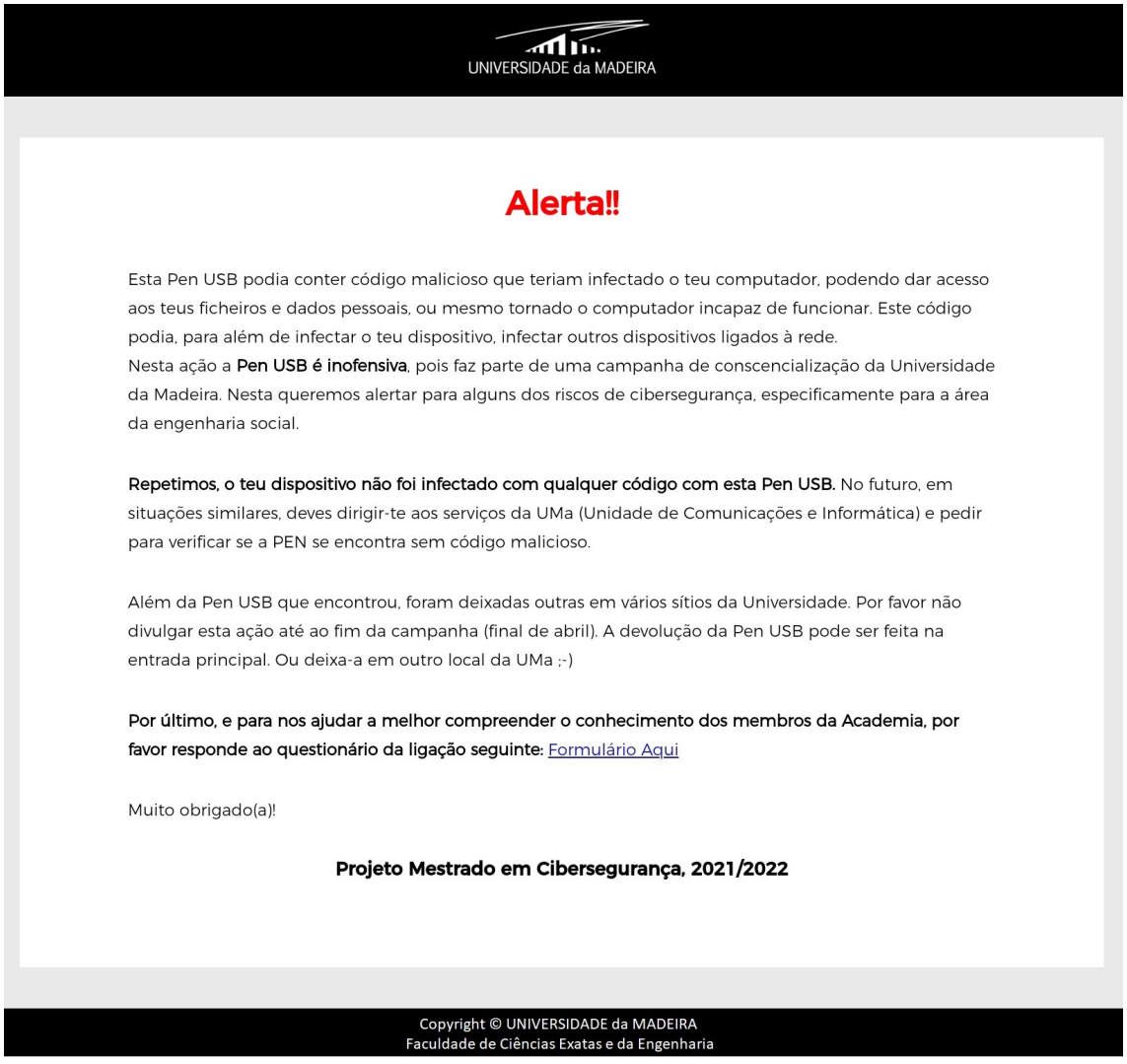

Figura 79: Página de alerta para o ataque via *pens USB*.

Figura 80: Primeira parte da página informativa para segundo ataque de *phishing*.

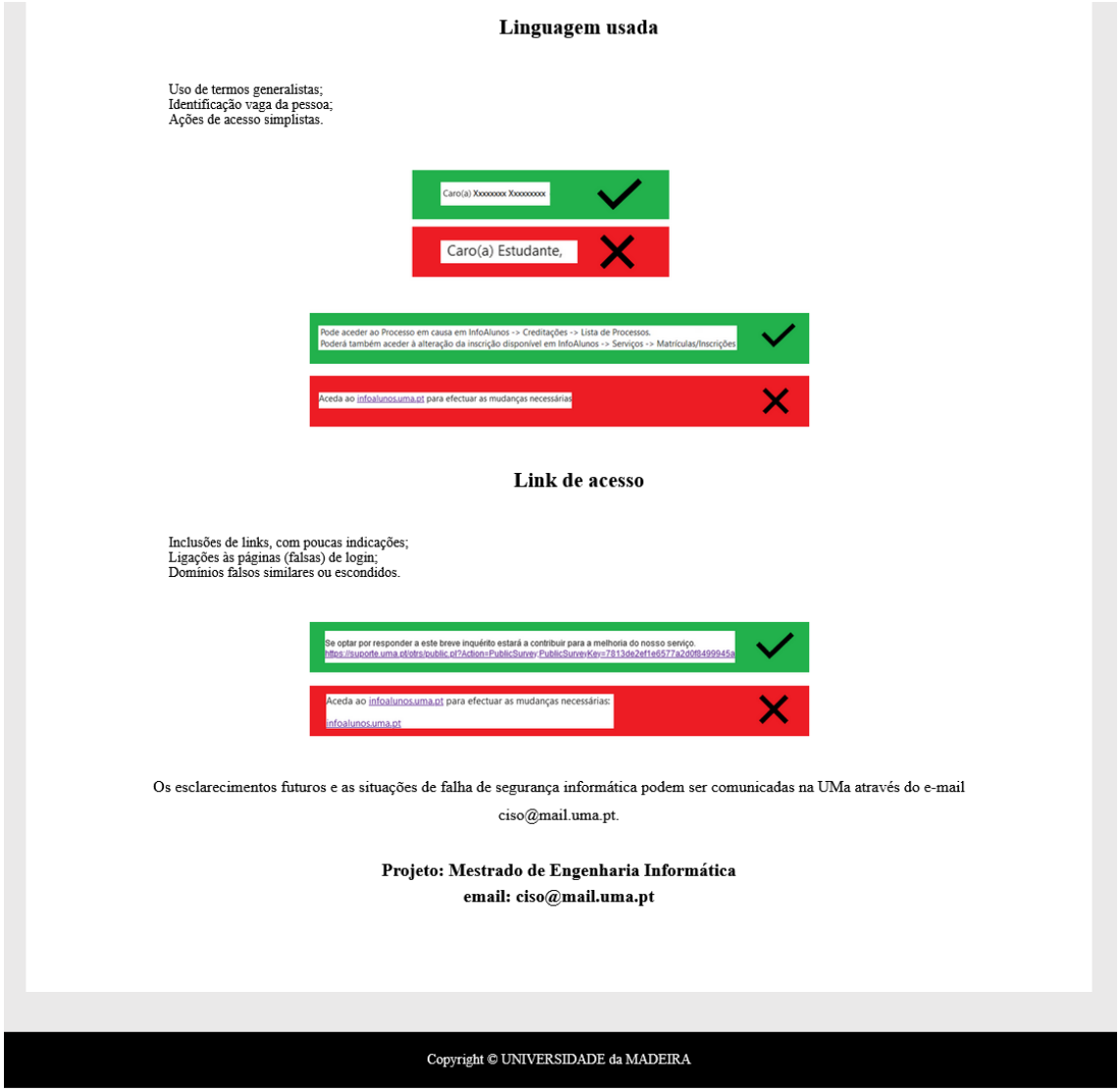

Figura 81: Segunda parte da página informativa para segundo ataque de *phishing*.

Anexos D - Questionário do Ataque de *Pens USB*

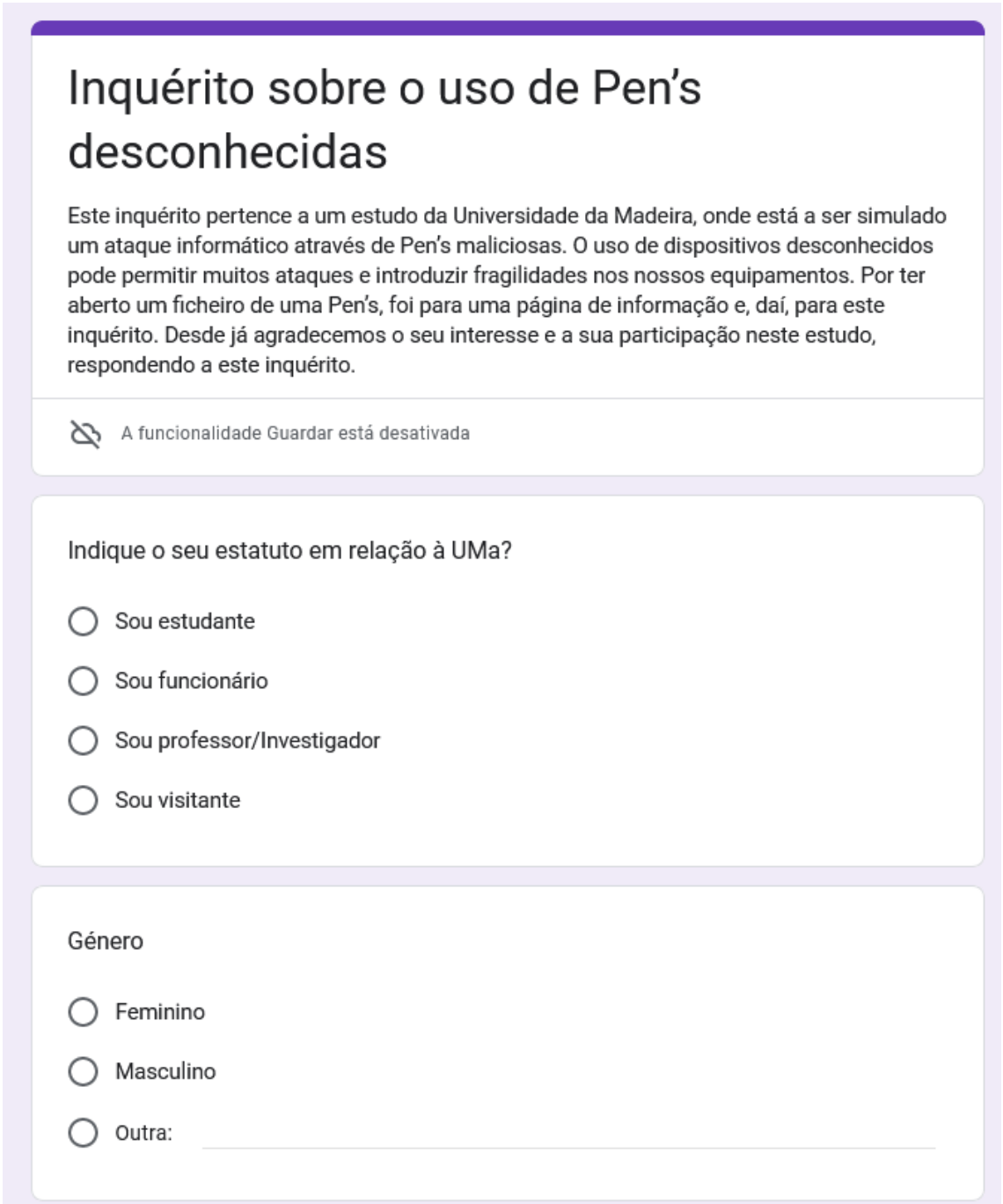

Figura 82: Perguntas um à três do questionário.

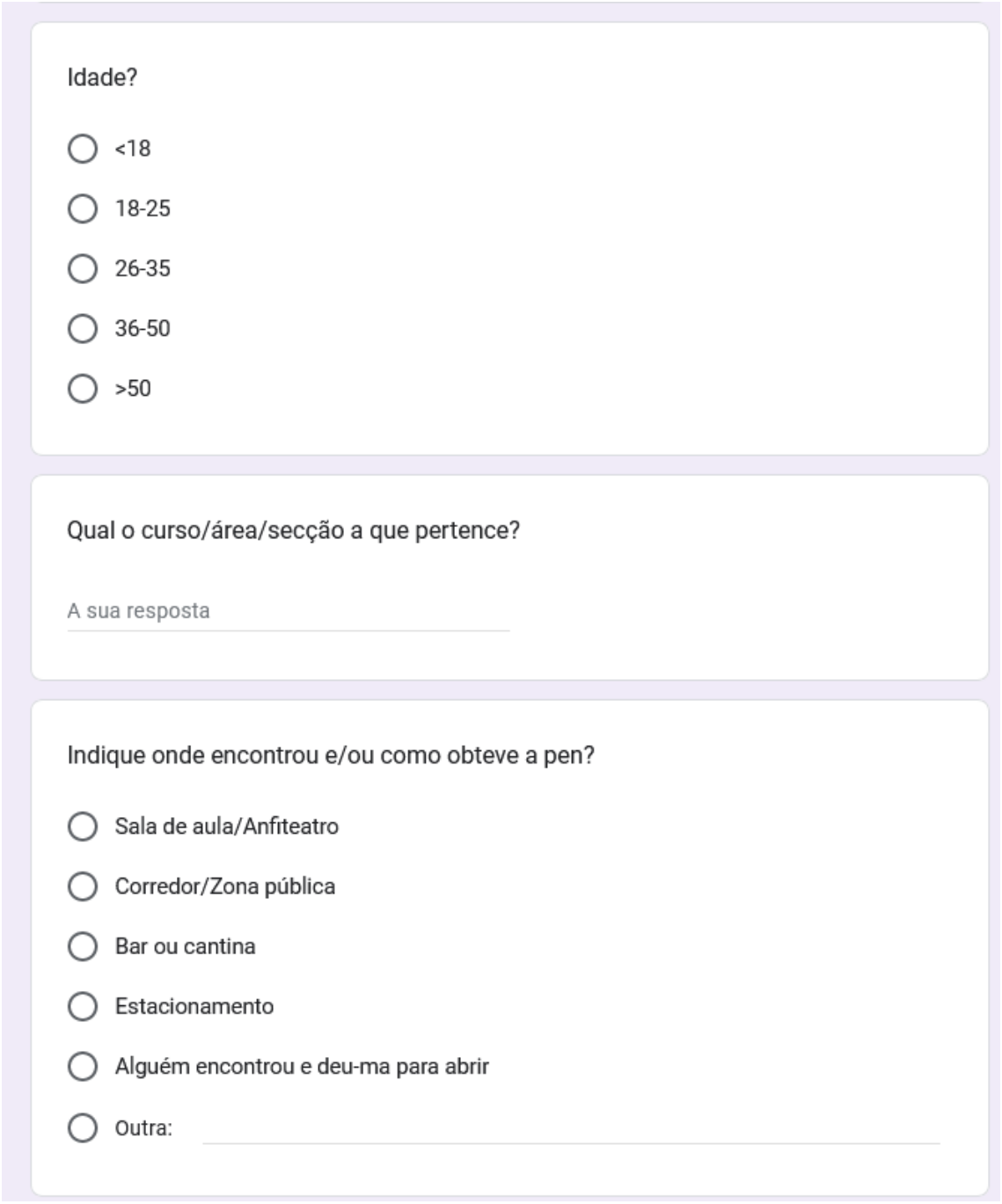

Figura 83: Perguntas quatro à seis do questionário.

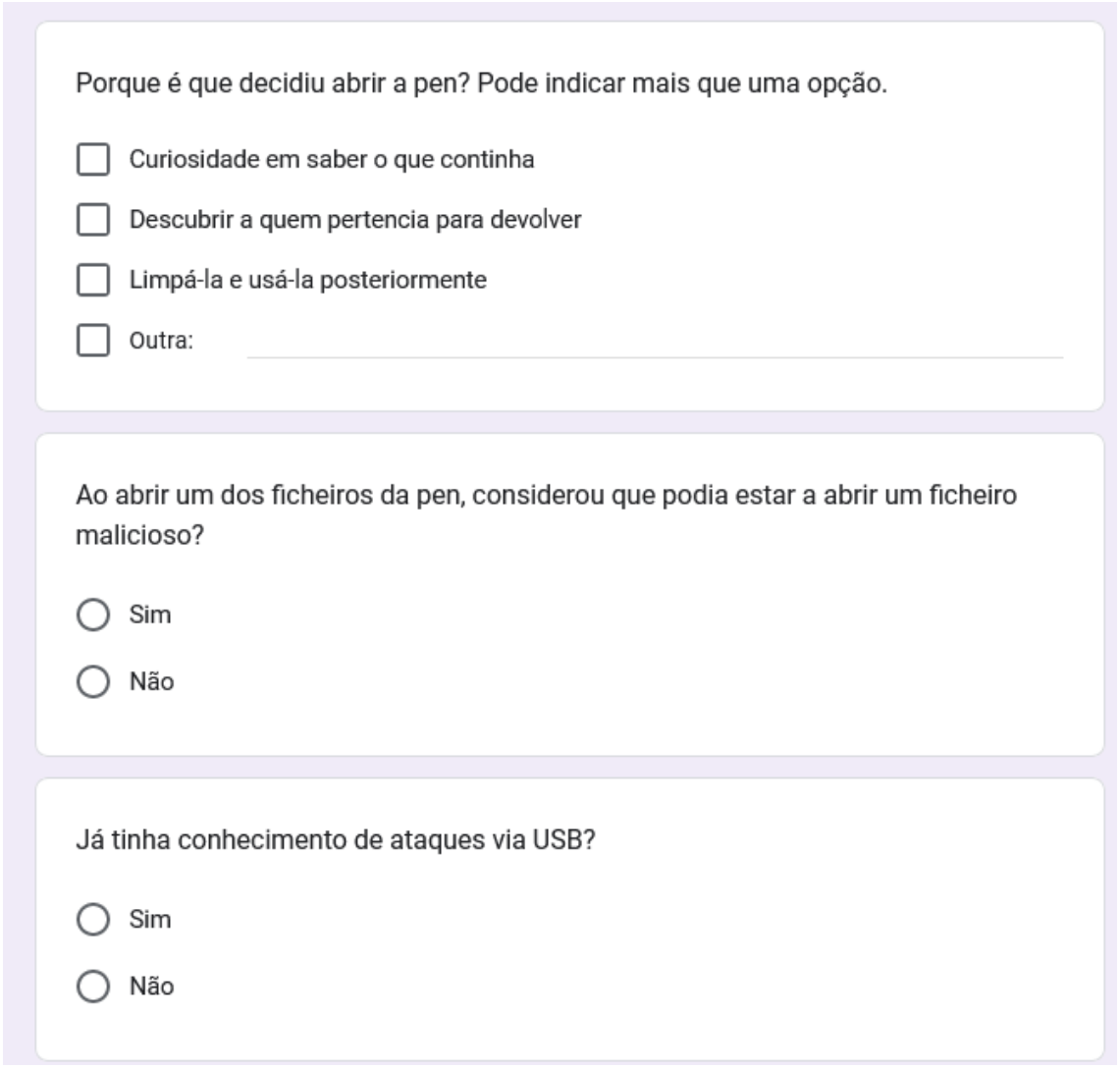

Figura 84: Perguntas sete à nove do questionário.

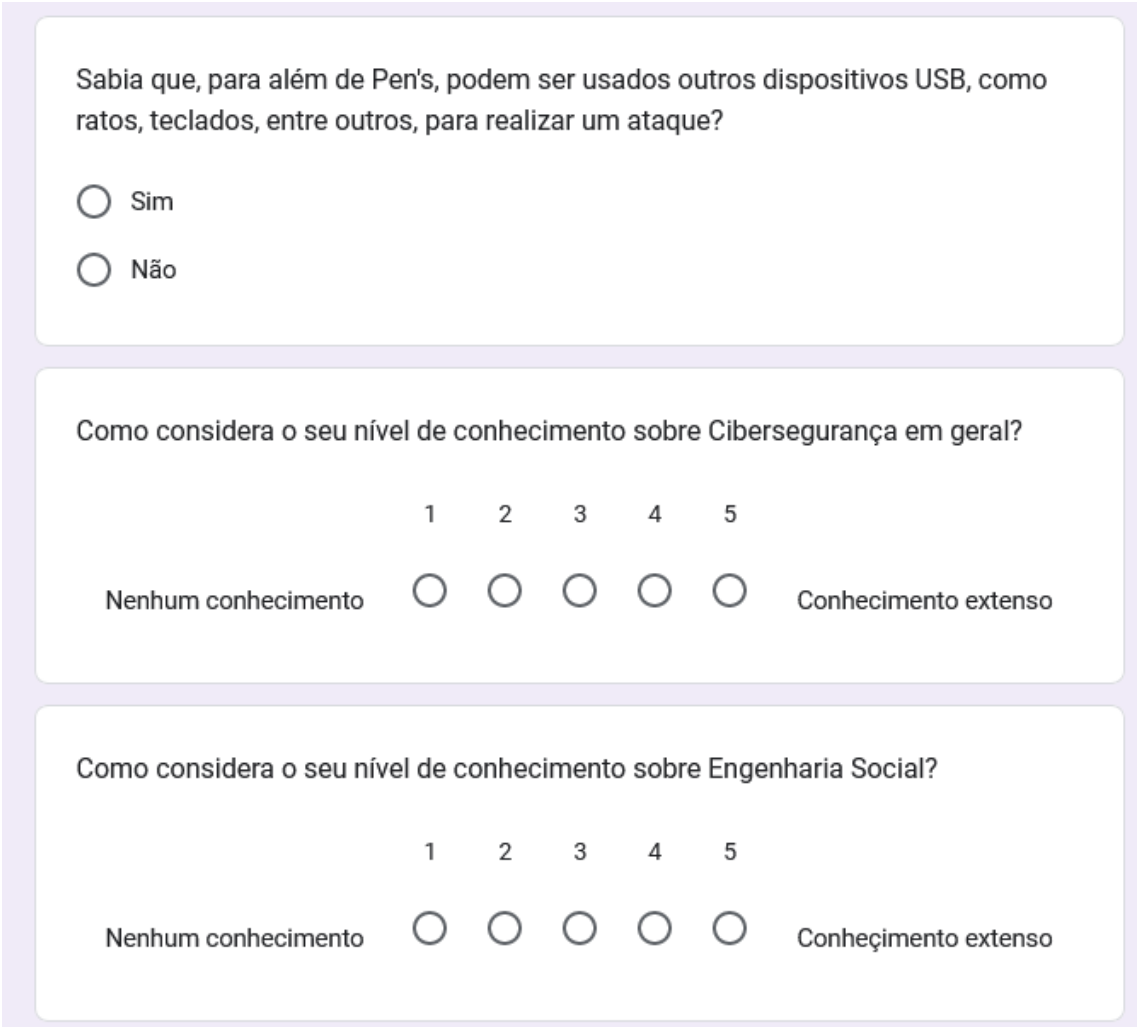

Figura 85: Perguntas dez à doze do questionário.

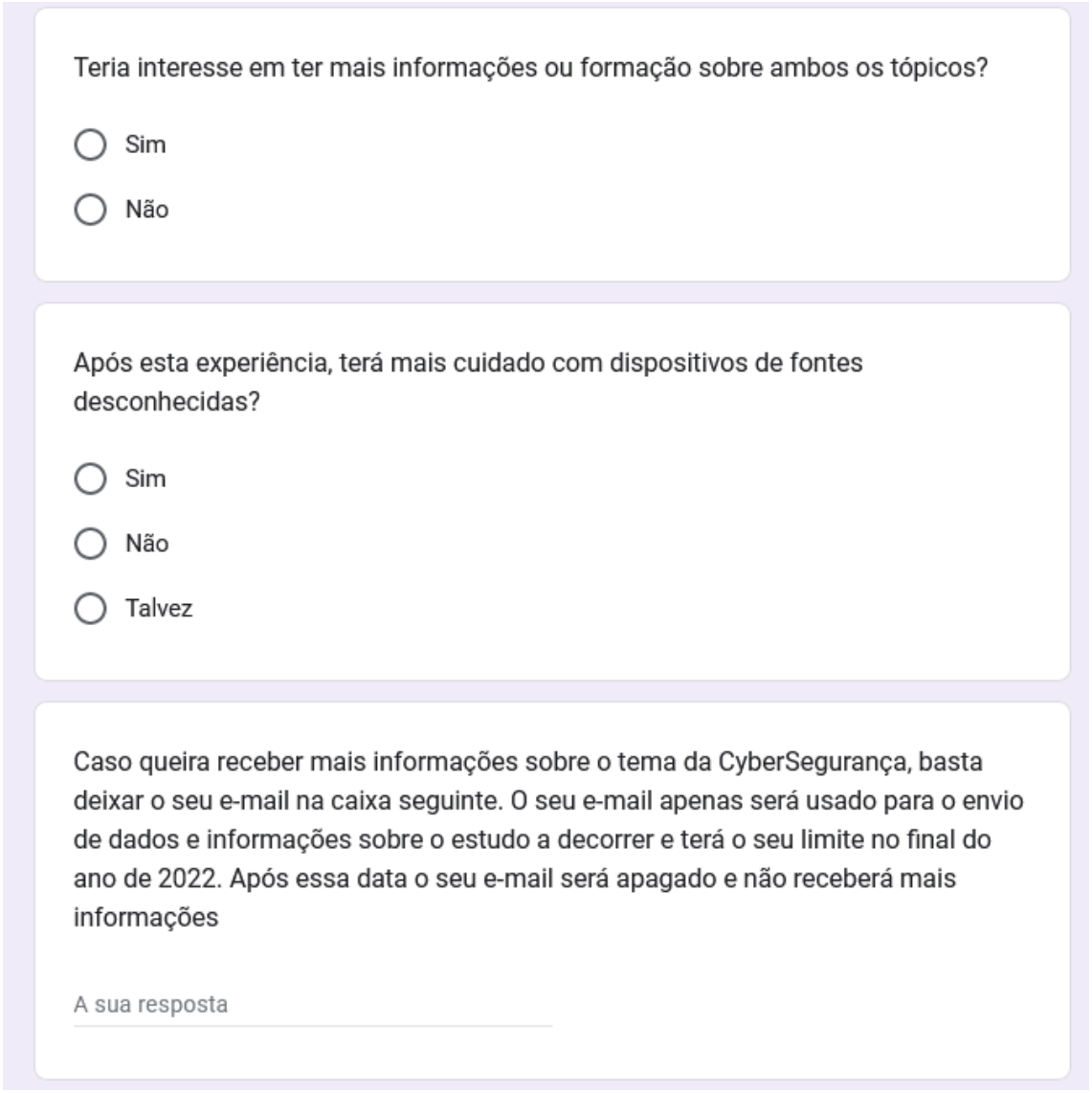

Figura 86: Perguntas treze à quinze do questionário.